

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-204698  
(43)Date of publication of application : 09.08.1996

(51)Int.Cl. H04L 9/00  
H04L 9/10  
H04L 9/12  
G06F 15/00  
G09C 1/00

(21)Application number : 07-008941  
(22)Date of filing : 24.01.1995

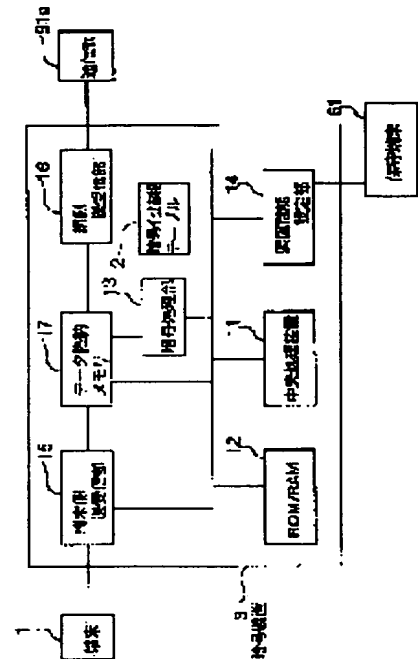
(71)Applicant : MITSUBISHI ELECTRIC CORP  
(72)Inventor : TOKINIWA YASUHISA  
WATANABE AKIRA  
SENOO SHOICHIRO  
YOKOYAMA YUKIO  
NAGASHIMA NORIMITSU

## (54) CIPHERING DEVICE

### (57)Abstract:

**PURPOSE:** To attain communication with a ciphering key corresponding to sets of a terminal address and a data class in the data transmission reception between terminal equipments by using a terminal address of a communication opposite party and a registered ciphering key so as to apply ciphering processing to data included in the communication information.

**CONSTITUTION:** A ciphering information table 2 provided corresponding to a ciphering device 3 stores an IP(Internet Protocol) address of a communication opposite party, a data class and a ciphering key with cross reference. Then the ciphering device 3 decodes a TCP(Transmission Control Protocol) data part of an IP packet with the ciphering key registered in the ciphering information table 2 based on sets of the IP address and the data class when sets matching with those of the transmitter IP address and the data class in the received IP packet are in existence in the ciphering information table 2 and gives the IP packet to the terminal equipment. When the same sets are not in existence in the table 2, the device 3 does not conduct decoding and gives the IP packet to the terminal equipment.



## LEGAL STATUS

[Date of request for examination]  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-204698

(43)公開日 平成8年(1996)8月9日

(51)IntCl. <sup>8</sup>		識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L	9/00				
	9/10				
	9/12				
G 0 6 F	15/00	3 3 0 Z	9364-5L		

H04L 9/00

$$Z$$

審査請求 未請求 請求項の数18 OL (全 32 頁) 最終頁に続く

(21)出願番号 特願平7-8941

(22)出願日 平成7年(1995)1月24日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 時庭 康久

鎌倉市大船五丁目1番1号 三菱電機株式  
会社通信システム研究所内

(72)発明者 渡辺 晃

鎌倉市大船五丁目1番1号 三菱電機株式  
会社通信システム研究所内

(72)発明者 妹尾 尚一郎

鎌倉市大船五丁目1番1号 三菱電機株式  
会社通信システム研究所内

(74)代理人 弁理士 高田 守 (外4名)

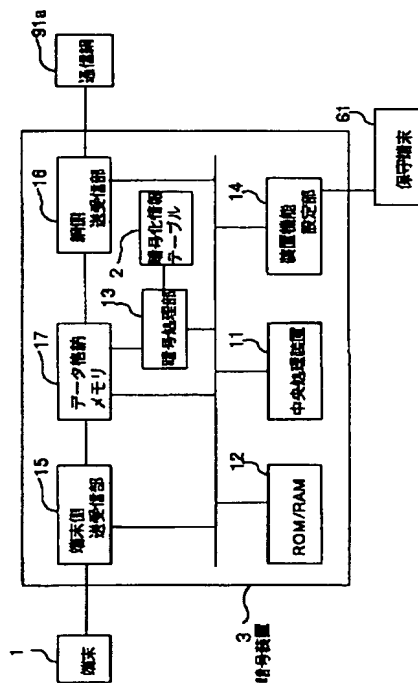
**最終頁に続く**

(54) 【発明の名称】 暗号装置

(57) 【要約】

【目的】 複数の端末間のデータ送受信において端末アドレスとデータ種別の組に対応した暗号鍵で通信できる暗号装置を得る。

【構成】 通信相手の端末アドレス、データ種別および暗号鍵を関連づけて登録する暗号化情報登録手段を設け、端末からの通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力し、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵とを用いて、通信情報に含まれるデータを暗号処理して出力する。



## 【特許請求の範囲】

【請求項 1】 以下の構成要素を有する暗号装置。

1. 通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力する入力手段、
2. 前記通信相手の端末アドレス、前記データ種別および暗号鍵を関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて前記通信情報に含まれるデータを暗号処理する暗号処理手段、
4. 前記暗号処理した前記通信情報を出力する出力手段。

【請求項 2】 以下の構成要素を有する暗号装置。

1. 通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段、
2. 前記通信相手の端末アドレスと複数の暗号鍵を関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる通信相手の端末アドレスに対応して前記暗号化情報登録手段に登録されている前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理する暗号処理手段、
4. 前記暗号処理した前記通信情報を出力する出力手段。

【請求項 3】 前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記通信相手の端末アドレスおよび複数の暗号鍵の他に前記データ種別を関連づけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの他に前記データ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項 2 に記載の暗号装置。

【請求項 4】 以下の構成要素を有する暗号装置。

1. 送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力する入力手段、
2. 前記送信元端末アドレス、前記宛先端末アドレスおよび暗号鍵を関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて前記通信情報に含まれるデータを暗号処理する暗号処理手段、
4. 前記暗号処理した前記通信情報を出力する出力手段。

【請求項 5】 以下の構成要素を有する暗号装置。

1. 第 1 の通信網および第 2 の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段、
2. 前記送信元端末アドレス、前記宛先端末アドレスおよび暗号鍵を関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して前記暗号化情報登録手段に登録

されている前記暗号鍵を用いて、前記第 2 通信網からの前記通信情報に含まれるデータを暗号化または、前記第 1 通信網からの前記通信情報に含まれるデータを復号する暗号処理手段、

4. 前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項 6】 前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記送信元端末アドレス、前記宛先端末アドレス、および暗号鍵の他に前記データ種別を関連づけて登録し、前記暗号処理手段は前記送信元端末アドレスと前記宛先端末アドレスの他に前記データ種別にも対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項 4 または請求項 5 に記載の暗号装置。

【請求項 7】 以下の構成要素を有する暗号装置。

1. 通信相手の端末アドレスと暗号対象のデータを含む前記通信情報を入力する入力手段、
2. 前記通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる前記通信相手の端末アドレスに対応して前記暗号化情報登録手段に登録されている前記第一の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを暗号化または、前記第二の暗号鍵を用いて前記通信相手からの前記通信情報に含まれるデータを復号する暗号処理手段、
4. 前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項 8】 前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他に前記データ種別とを関連づけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの他に前記データ種別に対応して前記暗号化情報登録手段に登録されている前記第一の暗号鍵を用いて暗号化または、前記第二の暗号鍵を用いて復号することを特徴とする請求項 7 に記載の暗号装置。

【請求項 9】 以下の構成要素を有する暗号装置。

1. 通信相手の端末アドレス、データ種別と暗号対象のデータを含む前記通信情報を入力する入力手段、
2. 前記通信相手の端末アドレス、前記データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録する暗号化情報登録手段、
3. 前記通信情報に含まれる前記通信相手の端末アドレスと前記データ種別に対応して前記暗号化情報登録手段に登録されている前記第一の複数の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを複数回暗号化または、前記第二の複数の暗号鍵を用いて前記通信

相手からの前記通信情報に含まれるデータを複数回復号する暗号処理手段、

4. 前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項10】 前記暗号化情報登録手段は前記送信元端末アドレスと前記宛先端末アドレスに複数の暗号鍵を関連づけて登録し、前記暗号処理手段は前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理することを特徴とする請求項4に記載の暗号装置。

【請求項11】 前記暗号化情報登録手段は前記送信元端末アドレスと前記宛先端末アドレスに複数の暗号鍵を関連づけて登録し、前記暗号処理手段は前記複数の暗号鍵を用いて、前記第2通信網からの前記通信情報に含まれるデータを複数回暗号化または、前記第1通信網からの前記通信情報に含まれるデータを複数回復号することを特徴とする請求項5に記載の暗号装置。

【請求項12】 前記暗号化情報登録手段は前記通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録し、前記暗号処理手段は前記第一の複数の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを複数回暗号化または、前記第二の複数の暗号鍵を用いて前記通信相手からの前記通信情報に含まれるデータを複数回復号することを特徴とする請求項7に記載の暗号装置。

【請求項13】 以下の構成要素を有する暗号装置。

1. 送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力する入力手段、

2. 前記送信元端末アドレス、前記宛先端末アドレス、前記データ種別および複数の暗号鍵を関連づけて登録する暗号化情報登録手段、

3. 前記通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して前記暗号化情報登録手段に登録されている前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理する暗号処理手段、

4. 前記暗号処理した前記通信情報を出力する出力手段。

【請求項14】 前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁をデータ種別と前記暗号鍵に関連づけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁と前記データ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項1に記載の暗号装置。

【請求項15】 前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁を前記暗号鍵に関連づけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁に対応して前記暗号化情報

登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項2に記載の暗号装置。

【請求項16】 前記暗号化情報登録手段は複数桁からなる前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁を前記暗号鍵に関連づけて登録し、前記暗号処理手段は前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項4に記載の暗号装置。

【請求項17】 前記暗号化情報登録手段は複数桁からなる前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁を前記暗号鍵に関連づけて登録し、前記暗号処理手段は前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号化または復号することを特徴とする請求項5に記載の暗号装置。

【請求項18】 前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁を前記暗号鍵に関連づけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号化または復号することを特徴とする請求項7に記載の暗号装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、通信網における暗号通信に関するものである。

【0002】

【従来の技術】従来より暗号方式には秘密暗号方式と呼ばれるものがあり、例えば64ビットの鍵を用いたANSI（アメリカ規格協会）の標準であるDES（Data Encryption Standard）方式や日本電信電話株式会社の登録商標であるFEAL（Fast data Encipherment Algorithm）などがある。また、通信網における暗号通信に関する暗号装置や暗号通信方式として、宛先の端末に対応した鍵を用いた暗号通信について、特開昭61-81044、特開平4-86041、特開平4-297155、特開平4-326222、特開平5-244153などの数多くの例が考案されている。

図19は例えば特開平4-297155号公報に示された従来の暗号装置の実施例を示す構成図である。図19において、1は端末、3は暗号装置、702はアドレス情報を保持するアドレス保持部、703は第1分岐合成回路、704は変調復調器、705は第2分岐合成回路、707はトランシーバ、91aは通信網である。

【0003】次に動作について説明する。図20、図21は従来の暗号装置の処理手順を示す図である。端末1から暗号化の対象となるパケットの宛先アドレスとその暗号系列を表す暗号鍵をアドレス保持部702に送り、アドレス保持部702がその宛先アドレスと暗号鍵を対

応させてメモリに保持することによって初期設定を行う。

【0004】図20は送信の処理手順を示し、ステップ714で端末1が暗号装置3にパケットを送る。ステップ715で、暗号装置3の第1分岐合成回路703がアドレス保持部702にそのパケットの宛先が保持されているか参照し、ステップ716で、宛先アドレスが保持されているならば、ステップ717に進み、第1分岐合成回路703がパケットを変調復調器704に送る。ステップ735で変調復調器704がアドレス保持部702からパケットの宛先アドレスの暗号鍵を受け取り、ステップ736で、変調復調器704が暗号鍵に従ってパケットを暗号化し、ステップ719で、変調復調器704がそのパケットを第2分岐合成回路705に送りステップ721に進む。ステップ716で、アドレス保持部702に宛先アドレスが保持されていなければ、ステップ720に進み、第1分岐合成回路703がパケットを第2分岐構成回路705に送る。次に、ステップ721で、第2分岐合成回路705がパケットを通信網91aに送る。

【0005】図21は受信の処理手順を示し、ステップ724で、通信網91aから暗号装置3にパケットを送られ、ステップ725で、暗号装置3の第2分岐合成回路705がアドレス保持部702にパケットの送信元アドレスが保持されているか参照し、ステップ726で、送信元アドレスが保持されているならば、ステップ727に進み、第2分岐合成回路705がパケットを変調復調器704に送り、ステップ735で変調復調器704がアドレス保持部702からパケットの送信元アドレスの暗号鍵を受け取り、ステップ737で、暗号鍵に従って暗号を復号し、ステップ729で、復号されたパケットを第1分岐合成回路703に送り、ステップ731に進む。ステップ726で、アドレス保持部702に送信元アドレスが保持されていなければ730に進み、第2分岐合成回路705がパケットを第1分岐合成回路703に送り、ステップ731で、第1分岐合成回路703がパケットを端末1に送る。

【0006】通信網91aに接続された複数の端末1間の通信で、暗号装置3のパケット送受信において共通の暗号鍵を用いて前記暗号化・復号を行うことにより暗号閉域通信が可能となる。

【0007】

【発明が解決しようとする課題】従来の暗号装置は以上のように通信相手対応に暗号鍵を用いるので、ある相手端末にパケットを送る場合、データ種別に関係なくすべてのデータを同じ暗号鍵で暗号化・復号を行っていて、データ種別によっては暗号化する必要がないデータまで暗号化していたため、暗号化・復号に掛かる無駄な遅延時間が発生していた。また、複数の相手端末と暗号通信する場合、一つの暗号鍵を共用すると暗号鍵が漏れる可

能性が高まり、暗号鍵の強度が弱い欠点があった。また、相互に暗号通信の必要のない安全域のネットワークに属する端末と暗号通信を必要とする危険域のネットワークに属する端末が通信する場合、安全域のネットワーク内の端末ごとに暗号装置を設ければ暗号通信が可能であるが多くの費用を要した。

【0008】また、2つの端末間のパケットは、送信／受信に係わらず同一の暗号鍵を用いて暗号化・復号を行っていたので、どちらかの方向の暗号が破られれば、他方向の暗号が破られるため暗号強度が弱いという問題があった。また、端末アドレスの上位桁が同一の端末がネットワークまたはサブネットワークを構成し、ネットワーク内の各端末が同じ暗号鍵を用いて、他のネットワークの端末と暗号通信する場合でも、通信相手と暗号鍵との関係を示す情報を端末毎に登録しなければならず、保守の労力が大きかった。

【0009】この発明は前記のような問題点を解消するためになされたもので、第一の目的は、端末間のデータ送受信において端末アドレスとデータ種別の組に対応した暗号鍵で通信できる暗号装置を得ることを目的とする。

【0010】第二の目的は、端末間のデータ送受信において暗号強度の異なる鍵で通信できる暗号装置を得ることを目的とする。

【0011】第三の目的は、安全域内では暗号通信する必要のない通信網に属する端末が、暗号通信を必要とする危険域内の通信網に属する端末と通信する際、危険域内は暗号通信できる暗号装置を得ることを目的とする。

【0012】第四の目的は、端末間のデータ送受信において送信用と受信用とで別の暗号鍵で通信できる暗号装置を得ることを目的とする。

【0013】第五の目的は、一つの通信網に属している端末に暗号鍵を設定するための操作労力を軽減することを目的とする。

【0014】

【課題を解決するための手段】第一の発明に係わる暗号装置は、通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、データ種別および暗号鍵を関連づけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【0015】第二の発明に係わる暗号装置は、通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレスと複数の暗号鍵を関連づけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスに対応して暗号

化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【0016】第三の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスおよび複数の暗号鍵の他にデータ種別を関連づけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【0017】第四の発明に係わる暗号装置は、送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連づけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【0018】第五の発明に係わる暗号装置は、第1の通信網および第2の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連づけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて、第2通信網からの通信情報に含まれるデータを暗号化または、第1通信網からの通信情報に含まれるデータを復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【0019】第六の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、および暗号鍵の他にデータ種別を関連づけて登録し、暗号処理手段は送信元端末アドレスと宛先端末アドレスの他にデータ種別にも対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【0020】第七の発明に係わる暗号装置は、通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連づけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて通信相手への通信情報に含まれるデータを暗号化または、第二の暗号鍵を用いて通信相手からの通信情報に含まれるデータを復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【0021】第八の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他にデータ種別とを関連づけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて暗号化または、第二の暗号鍵を用いて復号するものである。

【0022】第九の発明に係わる暗号装置は、通信相手の端末アドレス、データ種別と暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【0023】第十の発明に係わる暗号化情報登録手段は、送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連づけて登録し、暗号処理手段は複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理するものである。

【0024】第十一の発明に係わる暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連づけて登録し、暗号処理手段は複数の暗号鍵を用いて、第2通信網からの通信情報に含まれるデータを複数回暗号化または、第1通信網からの通信情報に含まれるデータを複数回復号するものである。

【0025】第十二の発明に係わる暗号化情報登録手段は通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録し、暗号処理手段は第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号するものである。

【0026】第十三の発明に係わる暗号装置は、送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレス、データ種別および複数の暗号鍵を関連づけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

る。

【0027】第十四の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁をデータ種別と暗号鍵に関連づけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁とデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【0028】第十五の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【0029】第十六の発明に係わる暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【0030】第十七の発明に係わる暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号するものである。

【0031】第十八の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号するものである。

【0032】

【作用】第一の発明において、入力手段が通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段が通信相手の端末アドレス、データ種別および暗号鍵を関連づけて登録する。そして、暗号処理手段が、通信情報に含まれる通信相手の端末アドレスと、データ種別に対応して暗号化情報登録手段に登録されている暗号鍵とを用いて通信情報に含まれるデータを暗号処理し、出力手段が暗号処理した通信情報を出力する。

【0033】第二の発明において、入力手段は通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスと複数の暗号鍵を関連づけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理し、出力手段は暗号処理した通信情報を出力する。

【0034】第三の発明において、入力手段はデータ

種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスおよび複数の暗号鍵の他にデータ種別を関連づけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【0035】第四の発明において、入力手段は送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段が送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連づけて登録する。そして、暗号処理手段は通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理し、出力手段は暗号処理した通信情報を出力する。

【0036】第五の発明において、入力手段は第1の通信網および第2の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連づけて登録する。そして、暗号処理手段が通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて、第2通信網からの通信情報に含まれるデータを暗号化または、第1通信網からの通信情報に含まれるデータを復号し、出力手段が暗号化または復号した通信情報を出力する。

【0037】第六の発明において、入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、および暗号鍵の他にデータ種別を関連づけて登録し、暗号処理手段は送信元端末アドレスと宛先端末アドレスの他にデータ種別にも対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【0038】第七の発明において、入力手段は通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連づけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて通信相手への通信情報に含まれるデータを暗号化または、第二の暗号鍵を用いて通信相手からの通信情報に含まれるデータを復号し、出力手段は暗号化または復号した通信情報を出力する。

【0039】第八の発明において、入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他にデータ種別とを関連づけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて暗号化または、第二の

10

20

30

40

50

暗号鍵を用いて復号することを特徴とする。

【0040】第九の発明において、入力手段は通信相手の端末アドレス、データ種別と暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号し、出力手段は暗号化または復号した通信情報を出力する。

【0041】第十の発明において、暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連づけて登録し、暗号処理手段は複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する。

【0042】第十一の発明において、暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連づけて登録し、暗号処理手段は複数の暗号鍵を用いて、第2通信網からの通信情報に含まれるデータを複数回暗号化または、第1通信網からの通信情報に含まれるデータを複数回復号する。

【0043】第十二の発明において、暗号化情報登録手段は通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連づけて登録し、暗号処理手段は第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号する。

【0044】第十三の発明において、入力手段は送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、データ種別および複数の暗号鍵を関連づけて登録する。そして、暗号処理手段は通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理し、出力手段は暗号処理した通信情報を出力する。

【0045】第十四の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁をデータ種別と暗号鍵に関連づけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁とデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【0046】第十五の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は通信相手

の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【0047】第十六の発明において、暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【0048】第十七の発明において、暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号する。

【0049】第十八の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連づけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号する。

【0050】

【実施例】

実施例1. 本実施例は端末対応だけではなく、端末とデータ種別の組に対応して暗号鍵を設けようとするもので、暗号装置の構成を図1に示す。図において、1は端末、3は暗号装置、11は各種の演算制御を行う中央処理装置、12はプログラムおよびワーキング用のメモリとして使用するROM/RAM、13は暗号処理部で、暗号化情報テーブル2を保持しデータの暗号化/復号を行う。14は暗号鍵の設定を行う装置機能設定部、15は端末側送受信部、16は網側送受信部、17はデータ格納メモリ、61は暗号鍵を入力するために用いる保守端末、91aは通信網である。

【0051】図2は、暗号通信システムの構成例を示す図であり、図において、1a~1hは端末、3a~3eは端末1a~1e対応に設けた暗号装置、91aは通信網である。なお、183aは端末1a、1b、1cが所属している通信閉域であり、183bは端末1a、1b、1d、1eが所属している通信閉域である。図3は、送受信データとしてのIP(Internet Protocol)パケットの構成を示す図であり、図において、401は送信元IPアドレス部、402は宛先IPアドレス部、411はIPヘッダ部、412はIPデータ部、431はデータ種別を収容するデータ種別部、441はTCPヘッダ部、442はTCPデータ部、445はIPパケットである。

【0052】なお、端末を識別するための端末アドレスとして、ここではIPアドレスを用いて説明するがMAC(Media Access Control)アドレスや他のネットワークプロトコルのアドレスであって



もよい。また、IPアドレスは、TCP/IP (Transmission Control Protocol / Internet Protocol) の通信手順で用いられている端末を識別するための4バイトの情報である。また、データ種別部431には、データ種別が入るが、ユーザアプリケーションを識別するポート番号であってもよい。

【0053】図4は、暗号装置3対応に設けた暗号化情報テーブル2の内容を例示するもので、図において、2a~2eは暗号装置3a~3e対応に設けた暗号化情報10  
テーブルで、通信相手のIPアドレス、データ種別および暗号鍵を一組とし関連づけて記憶する。そして、通信相手のIPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2内にあるか調べ、あるならその組に対応する暗号鍵を用いて暗号化または復号することを意味し、一致するものがなければ、暗号化または復号しないことを意味する。暗号化情報テーブル2内の31a~31eは端末を識別するためのIPアドレスで、各々  
端末1a~1eが対応する。

【0054】326a、326bはデータ種別で、341a、341bは暗号鍵である。本実施例ではデータ種別326aは暗号鍵341aに、データ種別326bは暗号鍵341bに対応させている。なお、図4は図2の通信網構成で暗号通信を行うために各暗号装置3の暗号化情報テーブル2に登録する内容を例示たもので、端末1aに対応する暗号化情報テーブル2aは暗号通信相手として端末1b、1c、1d、1eがあり、端末1bに対応するIPアドレス31bにデータ種別326aと暗号鍵341aおよびデータ種別326bと暗号鍵341bを割り当て、1cに対応するIPアドレス31cにデータ種別326a、暗号鍵341aを割り当てている。30

【0055】また、端末1d、1eに対応するIPアドレス31d、31eに、それぞれデータ種別326bと暗号鍵341bを割り当てている。以下同様に端末1b~1eに対応する暗号装置3b~3eの暗号化情報テーブル2b~2eには図4に示すIPアドレス、データ種別、暗号鍵を割り当てている。

【0056】次に、図5および図6を用いて端末1a、1b間を例にデータ送受信の動作を説明する。通信に先立ち暗号装置3aにおいて、通信相手のIPアドレス(31b)、データ種別、暗号鍵を組にして図4の暗号化情報テーブル2aに登録する。また、暗号装置3bにおいて、通信相手のIPアドレス(31a)、データ種別、暗号鍵を組にして暗号化情報テーブル2bに登録する。登録方法は図1に示す保守端末61を操作することにより、暗号装置3a、3bの装置機能設定部14を介して暗号処理部13が暗号化情報テーブル2a、2bに登録情報、即ち通信相手のIPアドレス(31b)、データ種別、暗号鍵を組にして記憶する。

【0057】次に、図5によりデータ送信の動作を自端 50

末1aから相手端末1b宛を例に説明する。自端末1aは、図4のIPパケットの送信元IPアドレス部401に自端末1aのIPアドレス31aを設定し、宛先IPアドレス部402に送信相手の端末1bのIPアドレス31bを設定し、データ種別部431にデータ種別(例えば326a)を設定し、IPパケット445を暗号装置3aへ送る。ステップ452で暗号装置3aが端末1aからIPパケット445を受け取る。ステップ453で、図1の暗号装置3aの端末側送受信部15は、前記のIPパケット445を受け取りデータ格納メモリ17に書き込み、中央処理装置11にIPパケット445を受け取ったことを伝える。ステップ454に進み、中央処理装置11は、暗号処理部13に対しIPパケット445を受け取ったことを伝え、暗号化を指示する。

【0058】そして、ステップ456に進み、暗号処理部13は、データ格納メモリ17からIPパケット445を読み取り、宛先IPアドレスとデータ種別の組と一致するものが図4の暗号化情報テーブル2a内にあるかサーチし、一致するものがない場合は、暗号化せずステップ458に進む。一致するものがあれば、ステップ457に進み、そのIPアドレスとデータ種別の組で登録しておいた暗号鍵でIPパケット445のTCPデータ部442を暗号化し、ステップ458に進む。ステップ458で、処理が終了したことを中央処理装置11に伝え、ステップ459に進む。ステップ459で中央処理装置11は、IPパケット445を通信網91aに送信するように網側送受信部16に指示する。そして、ステップ460で網側送受信部16は、データ格納メモリ17からIPパケット445を読み取り、通信網91aへ送る。

【0059】以上のように、送信するIPパケット445内の宛先IPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2内にあれば、その暗号化情報テーブル2がIPアドレスとデータ種別の組にして登録しておいた暗号鍵で、IPパケット445のTCPデータ部442を暗号化し送信する。同じものがなければ、暗号化せずIPパケット445を送信する。

【0060】次に、図6により、データ受信の動作を相手端末1aから自端末1b宛を例に説明する。ステップ463で自端末1bの暗号装置3bは、自端末宛のIPパケット445を通信網91aから受け取る。ステップ464で暗号装置3bの網側送受信部16は、前記のIPパケット445を受信しデータ格納メモリ17に書き込み、中央処理装置11に対してIPパケット445の受信を伝える。ステップ465で中央処理装置11は、暗号処理部13に対しIPパケット445の受信を伝え、復号を指示する。

【0061】ステップ467で暗号処理部13は、データ格納メモリ17からIPパケット445を読み取り、IPパケット445内の送信元IPアドレスとデータ種

別の組と一致するものが暗号化情報テーブル2 b内にあるかサーチし、一致するものがない場合は、復号せずステップ469に進む。一致するものがある場合は、ステップ468に進み、そのIPアドレスとデータ種別の組で登録しておいた暗号鍵でIPパケット445のTCPデータ部442を復号する。そして、ステップ469で、処理が終了したことを中央処理装置11に伝えステップ470に進む。ステップ470で中央処理装置11は、IPパケット445を自端末1bに送信するように端末側送受信部15に指示する。ステップ471で端末側送受信部15は、データ格納メモリ17からIPパケット445を読み取り自端末1bへ渡す。自端末1bは、暗号装置3bからIPパケット445を受け取る。

【0062】以上のように、暗号装置3は受信したIPパケット445内の送信元IPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2内にあれば、そのIPアドレスとデータ種別の組にして暗号化情報テーブル2に登録しておいた暗号鍵でIPパケット445のTCPデータ部442を復号し、IPパケット445を端末に渡す。同じものがない場合は、復号せずIPパケット445を端末に渡す。また、逆に端末1bから端末1aにデータを送る動作は上記の説明で端末1aと端末1bを置き換えたものと同様である。

【0063】次に、端末1aと端末1bとの間で異なるデータ種別326aと326bで暗号通信する例と、登録していないデータ種別326fを用いて通信する例を説明する。図4に示すように、あらかじめ暗号装置3aの暗号化情報テーブル2aに通信相手のIPアドレス31bとデータ種別326aと暗号鍵341aの組と、通信相手のIPアドレス31bとデータ種別326bと暗号鍵341bの組と、を登録しておく。また、暗号装置3bの暗号化情報テーブル2bに、通信相手のIPアドレス31aとデータ種別326aと暗号鍵341aの組と、通信相手のIPアドレス31aとデータ種別326bと暗号鍵341bの組と、を登録しておく。次に、端末1aがデータ種別326aで端末1bにデータを送信する例を説明する。

【0064】自端末1aは送信元IPアドレスに31aを、宛先IPアドレスに31bを、データ種別に326aを設定し、相手端末1b宛のIPパケット445を編集して、暗号装置3aに渡す。暗号装置3aは宛先IPアドレス31bとデータ種別326aが暗号化情報テーブル2aにあるか調べ、あるので、関連する暗号鍵341aで暗号化し通信網91aに送出する。端末1bの暗号装置3bは通信網91aから自端末宛IPパケット445を受信し、送信元IPアドレスとデータ種別326aの組と同じものがあるか調べ、暗号化情報テーブル2bにあるので、暗号装置3bはIPアドレスとデータ種別と組をなす暗号鍵341aで復号し、端末1bに渡す。

【0065】次に、端末1aが端末1bからデータを受信する例を説明する。端末1bは送信元IPアドレス31b、宛先IPアドレス31a、データ種別326aのIPパケット445を編集して、暗号装置3bに渡す。暗号装置3bは宛先IPアドレス31aとデータ種別326aの組と同じものが暗号化情報テーブル2bにあるか調べ、あるので、暗号装置3bはIPアドレスとデータ種別の組に対応する暗号鍵341aで暗号化し通信網91aに送出する。端末1aの暗号装置3aは通信網91aから自端末宛IPパケット445を受信し、送信元IPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2aにあるか調べ、あるので暗号装置3aはIPアドレスとデータ種別と組をなす暗号鍵341aで復号し、端末1aに渡す。

【0066】次に、端末1aがデータ種別326bで端末1bにデータを送信する例は、上記で用いたデータ種別326aを326bに置き換え同様の動作で通信ができる。ただし、暗号化・復号はデータ種別326bに対応して登録した暗号鍵341bを使用する。以上のように、同じ端末相互にデータ種別に応じ、異なる暗号鍵で暗号通信ができる。

【0067】次に、端末1aが未登録のデータ種別326fで端末1bにデータを送信する例を説明する。自端末1aは送信元IPアドレス31a、宛先IPアドレス31b、データ種別326fのIPパケット445を編集して、暗号装置3aに渡す。暗号装置3aは宛先IPアドレス31bとデータ種別326fの組と一致するものが暗号化情報テーブル2aにあるか調べ、ないので、暗号化せずに通信網91aに送出する。端末1bの暗号装置3bは通信網91aから自端末宛IPパケット445を受信し、送信元IPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2bにあるか調べ、ないので暗号装置3bは復号せず端末1bに渡す。

【0068】次に、端末1aが端末1bからデータを受信する例を説明する。端末1bは送信元IPアドレス31b、宛先IPアドレス31a、データ種別326fのIPパケット445を編集して、暗号装置3bに渡す。暗号装置3bは宛先IPアドレス31aとデータ種別326fの組と一致するものが暗号化情報テーブル2bにあるか調べ、ないので、暗号装置3bは暗号化せず通信網91aに送出する。端末1aの暗号装置3aは通信網91aから自端末宛IPパケット445を受信し、送信元IPアドレスとデータ種別の組と一致するものが暗号化情報テーブル2aにあるか調べ、ないので暗号装置3aは復号せず端末1aに渡す。

【0069】以上、2つの端末間で、データ種別によって異なる暗号で通信ができるので暗号強度が増す。また、暗号通信の必要がなければ未登録のデータ種別を用いることにより暗号化せずに通信することもでき、暗号化・復号に掛かる無駄な遅延時間をなくすることができ

る。

【0070】次に、端末1aから、暗号装置3aが接続されていない端末1fとの通信について説明する。あらかじめ暗号化情報テーブル2aから端末1fのIPアドレス31fを除いておく。図5および図6で説明したように、端末1aが送信元IPアドレス31a、宛先IPアドレス31fのIPパケット445を編集して暗号装置3aに渡す。暗号装置3aは宛先IPアドレス31fが暗号化情報テーブル2aにあるか調べ、登録していないので一致するものがなく暗号装置3aは暗号化せず送信する。次は逆に端末1fからの端末1a宛のIPパケット445を受信した暗号装置3aは暗号化情報テーブル2aに送信元IPアドレス31fがないので復号せずに受信したIPパケット445を端末1aに渡す。従って、暗号装置3を介して通信網91aに接続された端末1と暗号装置3を介さず直接通信網91aに接続された端末1間でも暗号化せずに通信できる。

【0071】図4のようにIPアドレス、データ種別、暗号鍵の組が登録されている状態で図2の通信網構成なら、上記の動作原理から端末1a、1b、1c、は同じデータ種別326aを使って相互に暗号通信ができ、端末1a、1b、1d、1eは同じデータ種別326bを使って相互に暗号通信ができる。従って、図2に示す通信閉域183a、183bのように端末相互に同一データ種別を用いた暗号通信の通信閉域を構成できる。また、端末1d、1eと端末1cは通信相手のIPアドレスが登録されていないので、相互に暗号化せずに通信できる。また、暗号装置3が接続されていない端末1f～1hは他の端末1a～1hと暗号化せずに通信できる。

【0072】なお、データ種別を同じにして暗号鍵を共有する例を示したが、データ種別は端末におけるデータ送受信の要求元のアプリケーションプログラムを識別するものであってもよい。また、上記実施例ではTCP/IPの通信手順の場合について説明したが、IPX (Internet Packet Exchange) やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。また、端末1と暗号装置3は1対1に接続している例を示したが暗号装置3に複数台の端末1を接続しても同様の効果を奏する。

【0073】暗号装置3に複数の端末1を接続する方法として、受信のときはIPパケット445の宛先IPアドレス部402にもとずいて、送信のときは送信元IPアドレス部401にもとずいて暗号装置3に収容される端末1を識別することにより暗号通信が可能である。たとえば、あらかじめ宛先アドレス、送信元アドレスと暗号鍵の組み合わせを暗号化情報テーブル2に登録しておく。ただし、宛先アドレスまたは送信元アドレスには暗号装置3に収容される端末1のアドレスを登録する。

【0074】端末1からIPパケット445を受信したとき、そのIPパケット445の宛先アドレスと送信元

アドレスが暗号化情報テーブル2に登録されていれば、宛先アドレスと送信元アドレスに関連して登録されている暗号鍵でIPパケット445のIPデータ部412を暗号化し、通信網91aに送信する。逆に、通信網91aから受信したIPパケット445の宛先アドレスと送信元アドレスが暗号化情報テーブル2に登録されていれば、宛先アドレスと送信元アドレスに関連して登録されている暗号鍵でIPパケット445のIPデータ部412を復号し、宛先アドレスの示す端末1へ受信したIPパケット445を渡す。

【0075】また、データ種別により使用する暗号鍵を変えるには、あらかじめ宛先アドレス、送信元アドレス、データ種別および暗号鍵の組み合わせを暗号化情報テーブル2に登録しておく。以下同様に、端末1からIPパケット445を受信したとき、そのIPパケット445の宛先アドレス、送信元アドレスおよびデータ種別が暗号化情報テーブル2に登録されていれば、宛先アドレス、送信元アドレスおよびデータ種別に関連して登録されている暗号鍵でIPパケット445のTCPデータ部442を暗号化し、通信網91aに送信する。逆に、通信網91aから受信したIPパケット445の宛先アドレス、送信元アドレスおよびデータ種別が暗号化情報テーブル2に登録されていれば、宛先アドレス、送信元アドレスおよびデータ種別に関連して登録されている暗号鍵でIPパケット445のTCPデータ部442を復号し、宛先アドレスの示す端末1へ受信したIPパケット445を渡す。以上により暗号装置3に複数の端末1を接続することができ、データ種別によって暗号鍵を変えることができる。

【0076】次に、上記例では、通信相手のIPアドレスをもとに使用する暗号鍵を決めていたが、IPアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、IPアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。ここで、図18はIPアドレス403の構成を示す図で、404はIPアドレスの上位桁で、ネットワークまたはサブネットワークのアドレスを示す。405はそのネットワーク内の端末識別子を示す。

【0077】そして、上記実施例の図4の暗号化情報テーブルのIPアドレスとデータ種別の組で一致するものをサーチする場合、IPアドレス一致の判定の代わりにネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。即ち、図5のステップ456および図6のステップ467においてIPアドレス一致の判定の代わりにネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属す

る端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるIPアドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0078】実施例2. 本実施例は、複数の暗号鍵を用いて暗号強度の強い通信を行なおうとするものである。図1は暗号装置の構成を示し、図2は通信システムの構成例を示し、図3は送受信データの構成を示すが、実施例1と同一で説明を省略する。図7は、暗号装置3対応に設けた暗号化情報テーブル2の内容を例示するものであり、実施例1の図4とは異なる。図7において、2a

～2eは暗号装置3a～3e対応に設けた暗号化情報テーブル2で、通信相手のIPアドレス、暗号鍵有効情報、第1暗号鍵、第2暗号鍵を一組として関連づけて記憶する。31a～31eはそれぞれ端末1a～1eのIPアドレスである。

【0079】また、341cおよび341dは暗号鍵である。そして、327a、327b、327cは暗号鍵有効情報に設定する値で、複数の暗号鍵を使用するか否かと、使用するなら鍵を使う順番を指定するものである。どの鍵を使うかは暗号化情報テーブル2の指定による。即ち、図7の例で、暗号鍵有効情報の値が327a

なら第1暗号鍵と第2暗号鍵が有効で、暗号化には第1暗号鍵の次に第2暗号鍵を用いることを、復号には逆に第2暗号鍵の次に第1暗号鍵を用いることを意味する。暗号鍵有効情報の値が327bなら第1暗号鍵のみが有効で、暗号化・復号に第1暗号鍵を用いることを意味し、暗号鍵有効情報の値が327cなら第2の暗号鍵のみが有効で、暗号化・復号に第2暗号鍵を用いることを意味する。

【0080】次に暗号装置3の送信動作について図8を用いて説明する。本図は実施例の図5と比較し、ステップ456、457をステップ455、473～477に置き換えたもので、ステップ455で送信IPパケット445の宛先IPアドレスに一致するものが図7の暗号化情報テーブル2内にあるかサーチして、一致するものがない場合は、復号せずステップ458に進む。一致するものがあれば、ステップ473に進み、その宛先IPアドレスと組をなす暗号鍵有効情報の値に従い、値が327bなら、ステップ474に進み第1暗号鍵を用いてIPデータ部412のデータを暗号化し、値が327c

ならステップ475に進み第2暗号鍵を用いてIPデータ部412のデータを暗号化し、値が327aならステップ476に進み、第1暗号鍵を用いてIPデータ部412のデータを暗号化し、ステップ477で、暗号化したIPデータ部412のデータをさらに第2暗号鍵を用いて暗号化し、ステップ458に進む。他の動作は実施例1の図5と同じで説明を省略する。

【0081】また、受信動作について図9を用いて説明する。本図は実施例の図6と比較し、ステップ467、468をステップ466、478～482に置き換えて

たもので、ステップ466で受信したIPパケット445内の送信元IPアドレスと同じものが暗号化情報テーブル2b内にあるかサーチし、一致するものがなければ復号せずステップ469に進む。一致するものがあれば、ステップ478に進み、そのIPアドレスと組をなす暗号鍵有効情報の値に従い、その暗号鍵有効情報の値が327bなら、ステップ479に進み第1暗号鍵を用いてIPデータ部412のデータを復号し、値が327cならステップ480に進み第2暗号鍵を用いてIPデータ部412のデータを復号し、値が327aならステップ481に進み、第2暗号鍵を用いてIPデータ部412のデータを復号し、ステップ482で、復号したIPデータ部412のデータをさらに第1暗号鍵を用いて、復号を行う。そして、ステップ469に進む。他の動作は実施例1の図6と同じで説明を省略する。

【0082】第1暗号鍵と第2暗号鍵を使って端末1aから端末1bへ送信する例を説明する。通信に先立ち、第1暗号鍵と第2暗号鍵を使って暗号通信するよう暗号鍵有効情報に327aを登録する。即ち、図7のようにあらかじめ暗号化情報テーブル2aのIPアドレスに31b、暗号鍵有効情報に327a、第1暗号鍵に341c、第2暗号鍵に341dを登録し、暗号化情報テーブル2bのIPアドレスに31a、暗号鍵有効情報に327a、第1暗号鍵に341c、第2暗号鍵に341dを登録しておく。次に、端末1aが送信元IPアドレス31a、宛先IPアドレス31bのIPパケット445を編集し、暗号装置3aに渡す。暗号装置3aは宛先IPアドレス31bに一致するものが暗号化情報テーブル2aにあるかサーチし、あればIPアドレス31bと組をなす暗号鍵有効情報の値327aに従い第1暗号鍵でIPデータ部412のデータを暗号化し、さらに第2暗号鍵で暗号化し、端末1b宛送信する。

【0083】次に、端末1bの暗号装置3dは通信網91aから宛先IPアドレス31bのIPパケット445を受信し、送信元IPアドレス31aに一致するものが暗号化情報テーブル1bにあるか調べ、あるので、送信元IPアドレス31aと組をなす暗号鍵有効情報の値327aに従い、第2暗号鍵でIPデータ部412のデータを復号した後、さらに第1暗号鍵で復号し端末1bに渡す。以下、第1暗号鍵のみを用いるときは暗号鍵有効情報に327bを、第2暗号鍵のみを用いるときは暗号鍵有効情報に327cを登録しておき、暗号化しないときはなにも登録しておかなければよい。

【0084】以上、本実施例では2つまでの鍵を用いた例を示したが2つ以上の複数鍵を用いてもよい。複数回暗号化すると暗号強度は増すが暗号化の演算量が増え暗号化・復号に時間が掛かるが、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。図7のようにIPアドレス、暗号鍵有効情報、第1暗号鍵、第2暗号鍵の組が登録され

ている状態で、図2の通信網構成なら、上記の動作原理から端末1a、1b、1cは第1暗号鍵341cを使って暗号通信ができ、端末1a、1b、1d、1eは第2暗号鍵341dを使って相互に暗号通信ができる。従って、端末相互に同一鍵を用いた暗号通信の通信閉域を構成できる。また、端末1d、1eと端末1cは通信相手のIPアドレスが登録されていないので相互に暗号化せずに通信できる。また、暗号装置3が接続されていない端末1f~1hは他の端末1a~1hと暗号化せずに通信できる。

【0085】また、本実施例は端末1のIPアドレス対応に暗号鍵を割り当てているが、実施例1のようにIPアドレスとデータ種別の組に対応して本実施例の暗号鍵を割り当て、暗号鍵に秘密鍵有効情報、第1暗号鍵、第2暗号鍵を用いて暗号強度に応じた暗号化を行うこともでき、2つ以上の複数鍵を用いて複数回暗号化・復号してもよい。また、暗号装置3に複数の端末1を接続する例においても、宛先アドレス、送信元アドレスの組、および宛先アドレス、送信元アドレスとデータ種別の組に対応して上記のように本実施例の暗号鍵を割り当ててもよい。なお、上記実施例では、暗号化・復号する送受信データの範囲をIPデータ部412に適用したが、TCPデータ部442に適用してもよい。また、上記実施例ではTCP/IPの通信手順の場合について説明したが、IPX (Internet Packet Exchange) やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。

【0086】また、端末1と暗号装置3は1対1に接続している例を示したが暗号装置3に複数台の端末1を接続しても同様の効果を奏する。次に、上記例では、通信相手のIPアドレスをもとに使用する暗号鍵を決めていたが、IPアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、IPアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【0087】上記実施例の図7の暗号化情報テーブルのIPアドレスと一致するものをサーチする場合、IPアドレス一致の判定の代わりに図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。即ち、送信の場合は図8のステップ455および受信の場合は図9のステップ466においてIPアドレス一致の判定の代わりにネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。他は上記実施例と同様である。このようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるIPアドレスの下位ビットを登録しなくてもよく、操作労力を軽減できる。

【0088】実施例3. 相互に暗号通信する必要のない

安全域のネットワークに属する端末が、暗号通信を必要とする危険域内の端末と通信する際、危険域内は暗号通信できるようにするものである。図1は暗号装置の構成を示し、図3は送受信データの構成を示すが、実施例1と同一で説明を省略する。図10は、第1通信網と第2通信網の間に暗号装置3mを設けた構成を示す図であり、図において、16は第1網側送受信部、18は第2網側送受信部、3mは暗号装置、91aは危険域の第1通信網、91bは安全域の第2通信網で、他は図1と同じで説明を省略する。

【0089】図11は暗号通信システムの構成例を示す図であり、図においては、91aは暗号通信の必要のある危険域の第1の通信網、91bは暗号通信の必要のない安全域の第2の通信網、1a~1hは第1の通信網91aに属する端末、1i~1lは第2の通信網91bに属する端末、3a~3eは各々端末1a~1eに対応して設けた暗号装置、3mは第1通信網91aと第2通信網91b間の暗号通信の中継を行う暗号装置である。図12は、暗号装置3ごとに設けた暗号化情報テーブル2の内容を例示するものであり、図において、2a、2b、2eは各々暗号装置3a、3b、3e対応に設けた暗号化情報テーブルで、内容は異なるが実施例2の図7に示す暗号化情報テーブル2と同じ構成である。

【0090】2mは暗号装置3mが暗号化・復号のために用いる暗号化情報テーブルで、第1の通信網側IPアドレス、第2の通信網側IPアドレス、暗号鍵有効情報、第1暗号鍵、第2暗号鍵を一組として関連づけて記憶する。31a、31b、31eは端末1a、1b、1eのIPアドレス、31i、31j、31kは端末1i、1j、1kのIPアドレスである。また、341eおよび341fは暗号化・復号で用いる暗号鍵、327bは実施例2で説明した暗号鍵有効情報で、第1暗号鍵のみが暗号化・復号に有効であることを示す。

【0091】通信に先立ち暗号装置3aにおいて、通信相手のIPアドレス(31i)、暗号鍵有効情報、第1暗号鍵、第2暗号鍵を組にして図12の暗号化情報テーブル2aに登録する。また、暗号装置3mにおいて、第1網側IPアドレス(31a)、第2網側IPアドレス(31i)、暗号鍵有効情報、第1暗号鍵、第2暗号鍵を組にして暗号化情報テーブル2mに登録する。

【0092】図13は第1通信網91aから第2通信網91bに中継する例を示す。この図により、データ送信の動作を相手端末1aから自端末1i宛を例に説明する。端末1aは送信元IPアドレス31a宛先IPアドレス31iのIPパケット445を編集し、暗号装置3aに渡す。暗号装置3aは実施例2の図8と同様に第1通信網91aへ暗号化したIPパケット445を送信する。ステップ463で暗号装置3mは、宛先IPアドレス31iのIPパケット445を第1通信網91aから受信する。

10

20

30

40

50

【0093】そしてステップ464に進み、図10の暗号装置3mの第1網側送受信部16は、前記のIPパケット445を受信しデータ格納メモリ17に書き込み、中央処理装置11に対してIPパケット445の受信を伝える。ステップ465で中央処理装置11は、暗号処理部13に対しIPパケット445の受信を伝え、復号を指示する。ステップ466で、暗号処理部13は、データ格納メモリ17からIPパケット445を読み取り、宛先IPアドレス31iと送信元IPアドレス31aの組と同じものが暗号化情報テーブル2m内にあるかサーチする。一致するものがなければステップ469に進む。

【0094】一致するものがあればステップ478に進み、IPアドレス31aとIPアドレス31iと組をなす暗号鍵有効情報の値に従い、その値が327bなら、ステップ479に進み第1暗号鍵を用いてIPデータ部412のデータを復号し、暗号鍵有効情報の値が327cならステップ480に進み第2暗号鍵を用いてIPデータ部412のデータを復号し、暗号鍵有効情報の値が327aならステップ481に進み、第2暗号鍵を用いてIPデータ部412のデータを復号し、ステップ482で、復号したIPデータ部412のデータをさらに第1暗号鍵を用いて、復号を行う。そして、ステップ469で処理が終了したことを中央処理装置11に伝える。ステップ470で、中央処理装置11は、IPパケット445を第2通信網91bに送信するように第2網側送受信部18に指示する。そしてステップ471で第2網側送受信部18は、データ格納メモリ17からIPパケット445を読み取り、第2通信網91bへ送る。端末1iは、第2通信網91bから宛先IPアドレス31iの自端末宛IPパケット445を受け取る。

【0095】次に、図14は第2通信網91bから第1通信網91aにデータを中継する例を示す。図14により、端末1aが端末1iからデータを受信する例について説明する。端末1iは、送信元IPアドレス31iで宛先IPアドレス31aのIPパケット445を編集し第2通信網91bへ送る。暗号装置3mは、ステップ452で宛先IPアドレス31aのIPパケット445を第2通信網91bから受け取る。ステップ453で、暗号装置3mの第2網側送受信部18は、前記のIPパケット445を受信しデータ格納メモリ17に書き込み、中央処理装置11に対してIPパケット445の受信を伝える。ステップ454で、中央処理装置11は、暗号処理部13に対しIPパケット445の受信を伝え、暗号化を指示する。

【0096】ステップ484で暗号処理部13は、データ格納メモリ17からIPパケット445を読み取り、宛先IPアドレス31aと送信元IPアドレス31iと一致するものが暗号化情報テーブル2m内にあるかサーチし、一致するものがなければステップ458に進む。一

致するものがあれば、ステップ473に進み、IPアドレス31aとIPアドレス31iと組をなす暗号鍵有効情報の値に従い、その値が327bなら、ステップ474に進み第1暗号鍵を用いてIPデータ部412のデータを暗号化し、暗号鍵有効情報の値が327cならステップ475に進み第2暗号鍵を用いてIPデータ部412のデータを暗号化し、暗号鍵有効情報の値が327aならステップ476に進み、第1の暗号鍵を用いてIPデータ部412のデータを暗号化し、ステップ477で、暗号化したIPデータ部412のデータをさらに第2の暗号鍵を用いて、暗号化を行う。そして、ステップ458に進み、処理が終了したことを中央処理装置11に伝える。ステップ459で中央処理装置11は、IPパケット445を第1通信網91aに送信するように第1網側送受信部16に指示する。

【0097】ステップ460で第1網側送受信部16は、データ格納メモリ17からIPパケット445を読み取り、第1通信網91aへ送る。暗号装置3aは、実施例2の図9と同様に第1通信網91aからIPパケット445を受け取り、IPデータ部412を復号して端末1aへ渡す。

【0098】以上により、第1通信網91a（危険域）からのIPパケット445を復号し第2通信網91b（安全域）へ中継し、逆に第2通信網91b（安全域）の端末からIPパケット445を暗号化し第1通信網91a（危険域）に中継できる。従って、安全域に属する複数の端末1対応に暗号装置3を設ける必要はなく、さらに暗号登録する必要もなく鍵の配布労力が省ける。図12のように暗号化情報テーブル2が登録されている状態で、図11の通信網構成なら、上記の動作原理から端末1a、1bと端末1i間は暗号鍵341eを用いて相互に危険域で暗号通信ができ、端末1e、1j、1k間は暗号鍵341fを用いて相互に危険域で暗号通信ができる。従って、端末1a、1b、1iは、共通の暗号鍵341eを用いた暗号通信の通信閉域を、端末1e、1j、1kは、共通の暗号鍵341fを用いた暗号通信の通信閉域を構成できる。

【0099】また、上記実施例では、暗号化・復号する送受信データの範囲をIPデータ部412に適用したが、TCPデータ部442に適用してもよい。そして、上記実施例ではTCP/IPの通信手順の場合について説明したが、IPX（Internet Packet Exchange）やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。さらに、上記例では暗号鍵として一つの鍵を用いる例を示したが、実施例2のように暗号鍵に秘密鍵有効情報、第1暗号鍵、第2暗号鍵を用いて暗号強度に応じた暗号化を行うこともでき、2つ以上の複数鍵を用いて複数回暗号化・復号してもよい。

【0100】またIPアドレスをもとに使用する暗号鍵を決めていたが、実施例1のようにIPアドレスとデー

10

20

30

40

50

タ種別に対応して本実施例の暗号鍵を割り当ててもよい次に、上記例では、通信相手のIPアドレスをもとに使用する暗号鍵を決めていたが、IPアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、IPアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【0101】上記実施例の図12の暗号化情報テーブル2mのIPアドレスと一致するものをサーチする場合、IPアドレス一致の判定の代わりに、図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。即ち、第2通信網内で同じ暗号鍵を用いる場合は図13のステップ466の宛先IPアドレスおよび図14のステップ484の送信元IPアドレス一致の判定の代わりに、図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。また、第1通信網内で同じ暗号鍵を用いる場合、図13のステップ466の送信元IPアドレスおよび図14のステップ484の宛先IPアドレス一致の判定の代わりに図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるIPアドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0102】実施例4. 本実施例は送信・受信に異なる暗号鍵を使えるようにしようとするものである。図1は暗号装置の構成を示し、図2は、暗号通信システムの構成例を示し、図3は送受信データの構成を示すが、実施例1と同一で説明を省略する。図15は暗号化情報テーブル2の内容を例示するものであり、実施例1の図4とは異なる。図において、2a~2eは暗号装置3a~3e対応に設けた暗号化情報テーブルで、通信相手IPアドレスと送信用暗号鍵、および受信用暗号鍵とを関連づけて記憶する。そして、送信・受信しようとするIPパケット445の宛先IPアドレス・送信元IPアドレスが暗号化情報テーブル2の通信相手IPアドレスに一致するものがあるか調べ、あるなら、その組に対応する送信用・受信用暗号鍵を用いて暗号化・復号し、一致するものがなければ、暗号化・復号せずにIPパケット445を送信・受信することを意味する。

【0103】例えば、図15の暗号装置3aの暗号化情報テーブル2aの暗号鍵341gはIPアドレス31aからIPアドレス31b宛の暗号化で用いる送信用暗号鍵で、暗号鍵341hは逆に端末1bから端末1a宛で復号に用いる受信用暗号鍵である。一方暗号装置3bの暗号化情報テーブル2bの暗号鍵341hはIPアドレス31bからIPアドレス31a宛のIPパケット44

5を暗号化するのに用いる送信用暗号鍵で、暗号鍵341gは逆に端末1aから端末1b宛でIPパケット445を復号するのに用いる受信用暗号鍵である。他の暗号鍵341i~341nも同様に送受別の鍵となるよう構成している。なお、31a~31eは端末1a~1eのIPアドレスである。

【0104】次に暗号装置3の送信動作について図16を用いて説明する。本図は実施例1の図5と比較し、ステップ456、457をステップ495、496に置き換えてたもので、ステップ495で送信IPパケット445の宛先IPアドレスと暗号化情報テーブル2内の通信相手IPアドレスとを比較し一致する通信相手IPアドレスをサーチして、一致するものがない場合は、暗号化せずステップ458に進む。一致するものがあれば、ステップ496に進み、その通信相手のIPアドレスに対応して登録しておいた送信用暗号鍵でIPパケット445のIPデータ部412を暗号化し、ステップ458に進む。他の動作は実施例1の図5と同じで説明を省略する。

【0105】また、受信動作について図17を用いて説明する。本図は実施例1の図6と比較し、ステップ467、468をステップ487、489に置き換えてたもので、ステップ487で受信IPパケット445の送信元IPアドレスと暗号化情報テーブル2内の通信相手のIPアドレスとを比較し一致する通信相手のIPアドレスの暗号化情報テーブル2内にあるかサーチして、一致するものがない場合は、復号せずステップ469に進む。一致するものがあれば、ステップ489に進み、その通信相手のIPアドレスに対応して登録しておいた受信用暗号鍵でIPパケット445のIPデータ部412を復号しステップ469に進む。他の動作は実施例1の図6と同じで説明を省略する。

【0106】次に、端末1aと端末1b間の送受信を例に暗号通信の動作を説明する。通信に先立ち図15の暗号装置3aの暗号化情報テーブル2aに通信相手IPアドレスに31b、送信用暗号鍵に341g、受信用暗号鍵に341hの組を登録し、暗号装置3bの暗号化情報テーブル2bに通信相手IPアドレスに31a、送信用暗号鍵に341h、受信用暗号鍵に341gの組を登録しておく。

【0107】そして、端末1aにおいて送信元IPアドレス31a、宛先IPアドレス31bのIPパケット445を編集し、暗号装置3aに渡すと、暗号装置3aは宛先IPアドレス31bに対応する送信用暗号鍵341gで暗号化し、通信網91aに送信する。一方、暗号装置3bは通信網91aから送信元IPアドレス31a、宛先IPアドレス31bのIPパケットを受信すると送信元IPアドレス31aに対応する受信用暗号鍵341gで復号し端末1bに渡す。次に端末1bが送信元IPアドレス31b、宛先IPアドレス31a、のIPパケ

ット445を編集し、暗号装置3bに渡すと、暗号装置3bは送信元IPアドレス31bと宛先IPアドレス31aの組に対応する暗号鍵341hで暗号化し、通信網91aに送信する。暗号装置3aが通信網91aから送信元IPアドレス31b、宛先IPアドレス31aのIPパケット445を受信すると、送信元IPアドレス31bに対応する受信用暗号鍵341hで復号し端末1aに渡す。

【0108】以上のように、端末1aから端末1bに送信するときは暗号鍵341gを用い、逆に端末1aが端末1bから受信するときは暗号鍵341hを用いるので送受信別の暗号鍵を用いて暗号通信ができる。従って、片方の暗号鍵が解読されても他方は解読されないの、従来例より暗号強度が増す。なお、本実施例では通信相手IPアドレスに送信用暗号鍵と受信用暗号鍵を割り当てているが、実施例1のデータ種別と本実施例の通信相手IPアドレスを組に対応して、送信用暗号鍵と受信用暗号鍵を割り当ててもよい。さらに、本実施例および上記の例で暗号鍵に実施例2の秘密鍵有効情報、第1暗号鍵、第2暗号鍵を割り当て暗号強度に応じた暗号化を行うこともでき、2つ以上の複数鍵を用いて複数回暗号化・復号してもよい。

【0109】また、上記実施例ではTCP/IPの通信手順の場合について説明したが、IPX (Internet Packet Exchange) やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。また、端末1と暗号装置3は1対1に接続している例を示したが暗号装置3に複数台の端末1を接続しても同様の効果を奏する。次に、上記例では、通信相手のIPアドレスをもとに使用する暗号鍵を決めていたが、IPアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、IPアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【0110】即ち、上記実施例の図15の暗号化情報テーブル2の通信相手IPアドレスと一致するものをサーチする場合、IPアドレス一致の判定の代わりに図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。例えば、送信の場合は図16のステップ495の通信相手IPアドレス一致の判定の代わりに、ネットワークを識別する通信相手IPアドレスの上位桁404を比較して一致の判定を行なう。また、受信の場合は図17のステップ487の通信相手IPアドレス一致の判定の代わりに、図18のネットワークを識別するIPアドレスの上位桁404を比較して一致の判定を行なう。他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるIP

アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0111】

【発明の効果】第一の発明においては、2つの端末間で、データ種別によって異なる暗号鍵を用いて通信できるので暗号強度が増す。

【0112】第二の発明においては、複数鍵を用いて複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【0113】第三の発明においては、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【0114】第四の発明においては、送信元アドレスと宛先アドレスの組み合わせに対応して暗号鍵を割り当てるので、送信と受信に別々の暗号鍵で通信でき暗号強度が増す。

【0115】第六の発明においては、危険域の第1の通信網からの受信情報を復号して安全域の第2の通信網へ中継し、逆に安全域の端末から受信情報を暗号化して危険域に中継するので、安全域に属する複数の端末対応に暗号装置を設ける必要はなく、さらに暗号登録する必要もなく鍵の配布労力が省ける。

【0116】第七の発明においては、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【0117】第八の発明においては、送信するときに用いる暗号鍵と受信するときに用いる暗号鍵を別にしたので、片方の暗号鍵が解読されても他方は解読されないの、従来例より暗号強度が増す。

【0118】第九の発明においては、送信と受信に別々にかつ、データ種別ごとに複数の暗号鍵を用いて複数回暗号化するのでさらに暗号強度が増す。

【0119】第十の発明においては、送信と受信に別々にかつ、複数の暗号鍵を用いて複数回暗号化するのでさらに暗号強度が増す。

【0120】第十一の発明においては、送信と受信に別々にかつ、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【0121】第十二の発明においては、宛先対応に複数鍵を用いて複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【0122】第十三の発明においては、送信元アドレス、宛先アドレスとデータ種別の組み合わせに対応して複数鍵を割り当て複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【0123】第十四の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減

10

20

30

40

50



減できる。

【0124】第十五の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0125】第十六の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0126】第十七の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0127】第十八の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【0128】

【図面の簡単な説明】

【図1】この発明の実施例1による暗号装置を示す構成図である。

【図2】この発明の実施例1による暗号通信システムを示す図である。

【図3】この発明の実施例1によるIPパケットの形式を示す図である。

【図4】この発明の実施例1による暗号化情報テーブルを示す図である。

【図5】この発明の実施例1による送信処理手順を示す図である。

【図6】この発明の実施例1による受信処理手順を示す図である。

【図7】この発明の実施例2による暗号化情報テーブルを示す図である。

【図8】この発明の実施例2による送信処理手順を示す図である。

【図9】この発明の実施例2による受信処理手順を示す図である。

【図10】この発明の実施例3による暗号装置を示す構成図である。

【図11】この発明の実施例3による暗号通信システムを示す図である。

【図12】この発明の実施例3による暗号化情報テーブルを示す図である。

【図13】この発明の実施例3による第2網側への中継

処理手順を示す図である。

【図14】この発明の実施例3による第1網側への中継処理手順を示す図である。

【図15】この発明の実施例4による暗号化情報テーブルを示す図である。

【図16】この発明の実施例4による送信処理手順を示す図である。

【図17】この発明の実施例4による受信処理手順を示す図である。

【図18】IPアドレス構成を示す図である。

【図19】従来の暗号装置を示す構成図である。

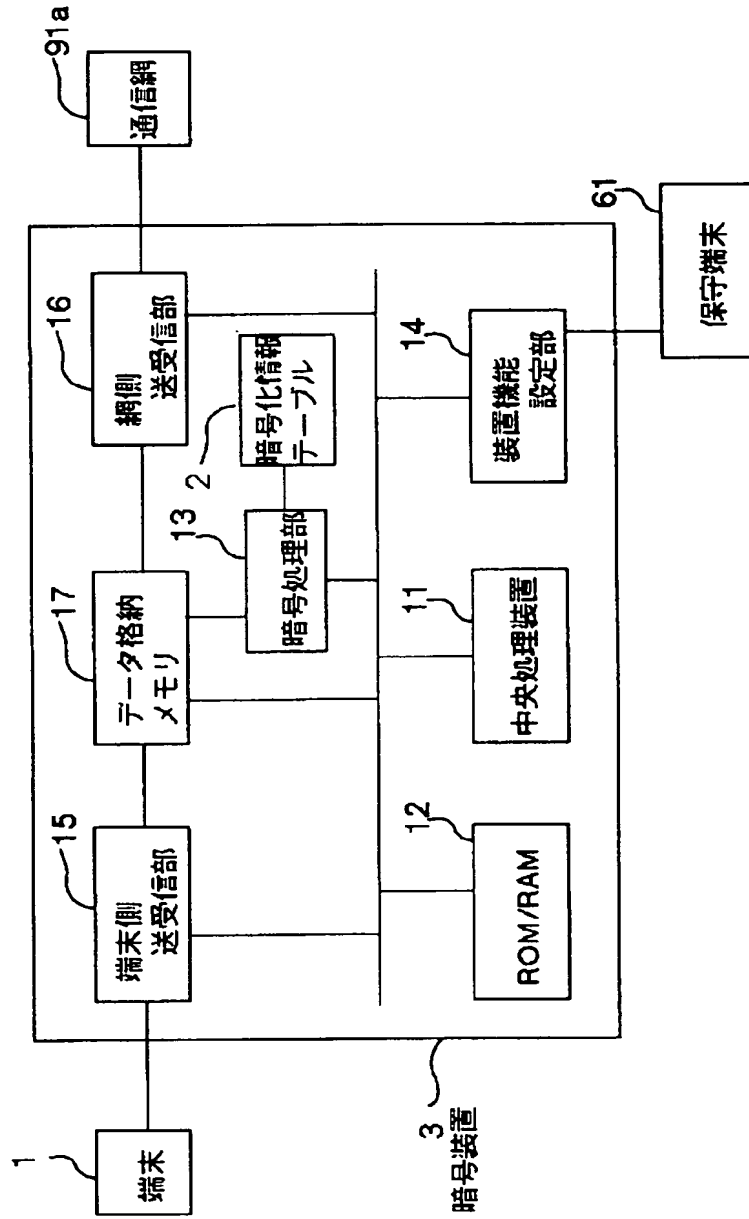
【図20】従来の実施例による送信処理手順を示す図である。

【図21】従来の実施例による受信処理手順を示す図である。

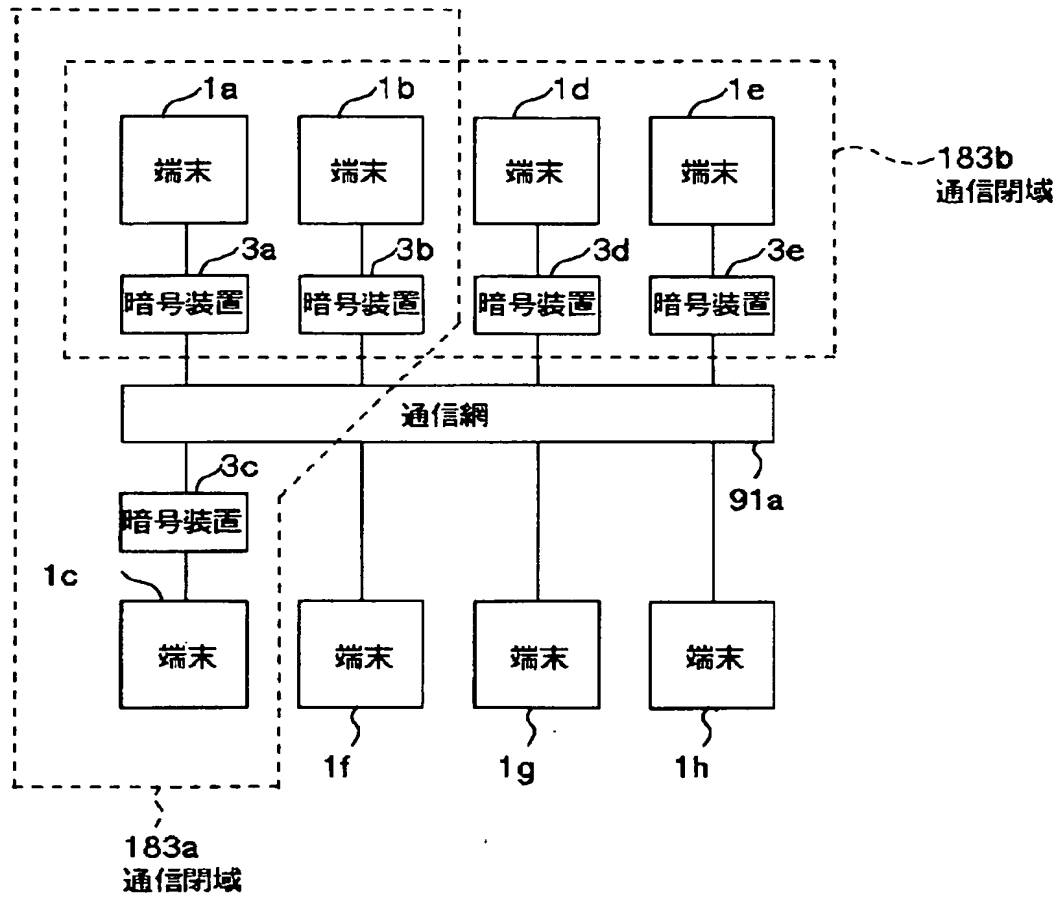
【符号の説明】

- 11 中央処理装置
- 12 ROM/RAM
- 13 暗号処理部
- 14 装置機能設定部
- 15 端末側送受信部
- 16 網側送受信部
- 17 データ格納メモリ
- 18 第2網側送受信部
- 3 暗号装置
- 3a~3e 暗号装置
- 3m 暗号装置
- 61 保守端末
- 91a 第1通信網
- 91b 第2通信網
- 1 端末
- 1a~1l 端末
- 2a~2e、2m 暗号化情報テーブル
- 31a~31e IPアドレス
- 31i~31k IPアドレス
- 326a~326b データ種別
- 327a~327c 暗号鍵有効情報
- 341a~341n 暗号鍵
- 401 送信元IPアドレス部
- 402 宛先IPアドレス部
- 404 IPネットワークアドレス
- 411 IPヘッダ部
- 412 IPデータ部
- 431 データ種別部
- 441 TCPヘッダ部
- 442 TCPデータ部
- 445 IPパケット

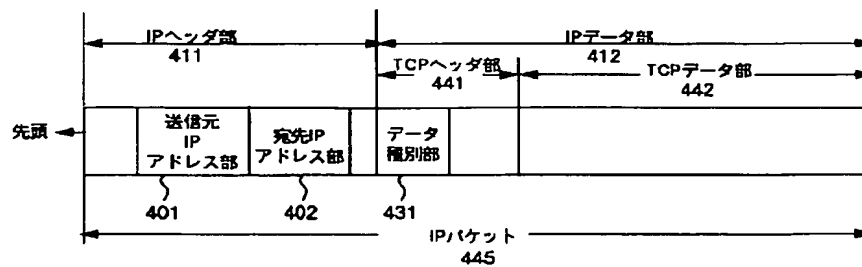
【図 1】



【図 2】



【図 3】



【図 4】

IPアドレス	データ種別	暗号鍵	2a 暗号化情報 テーブル
31b	326a	341a	
31b	326b	341b	
31c	326a	341a	
31d	326b	341b	
31e	326b	341b	

IPアドレス	データ種別	暗号鍵	2b 暗号化情報 テーブル
31a	326a	341a	
31c	326a	341a	
31a	326b	341b	
31d	326b	341b	
31e	326b	341b	

IPアドレス	データ種別	暗号鍵	2c 暗号化情報 テーブル
31a	326a	341a	
31b	326a	341a	

IPアドレス	データ種別	暗号鍵	2d 暗号化情報 テーブル
31a	326b	341b	
31b	326b	341b	
31e	326b	341b	

IPアドレス	データ種別	暗号鍵	2e 暗号化情報 テーブル
31a	326b	341b	
31b	326b	341b	
31d	326b	341b	

【図 7】

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2a 暗号化情報 テーブル
31b	327a	341c	341d	
31c	327b	341c	—	
31d	327c	—	341d	
31e	327c	—	341d	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2b 暗号化情報 テーブル
31a	327a	341c	341d	
31c	327b	341c	—	
31d	327c	—	341d	
31e	327c	—	341d	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2c 暗号化情報 テーブル
31a	327b	341c	—	
31b	327b	341c	—	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2d 暗号化情報 テーブル
31a	327c	—	341d	
31b	327c	—	341d	
31e	327c	—	341d	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2e 暗号化情報 テーブル
31a	327c	—	341d	
31b	327c	—	341d	
31d	327c	—	341d	

【図 12】

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2a 暗号化情報 テーブル
31b	327b	341e	—	
31i	327b	341e	—	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2b 暗号化情報 テーブル
31a	327b	341e	—	
31i	327b	341e	—	

IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2c 暗号化情報 テーブル
31j	327b	341f	—	
31k	327b	341f	—	

第1網側 IPアドレス	第2網側 IPアドレス	暗号鍵 有効情報	第1暗号鍵	第2暗号鍵	2m 暗号化情報 テーブル
31a	31i	327b	341e	—	
31b	31i	327b	341e	—	
31e	31j	327b	341f	—	
31e	31k	327b	341f	—	

【図 15】

通信相手 IPアドレス	送信用 暗号鍵	受信用 暗号鍵	2a 暗号化情報 テーブル
31b	341g	341h	
31c	341i	341j	

通信相手 IPアドレス	送信用 暗号鍵	受信用 暗号鍵	2b 暗号化情報 テーブル
31a	341h	341g	
31c	341k	341i	

通信相手 IPアドレス	送信用 暗号鍵	受信用 暗号鍵	2c 暗号化情報 テーブル
31a	341j	341i	
31b	341i	341k	

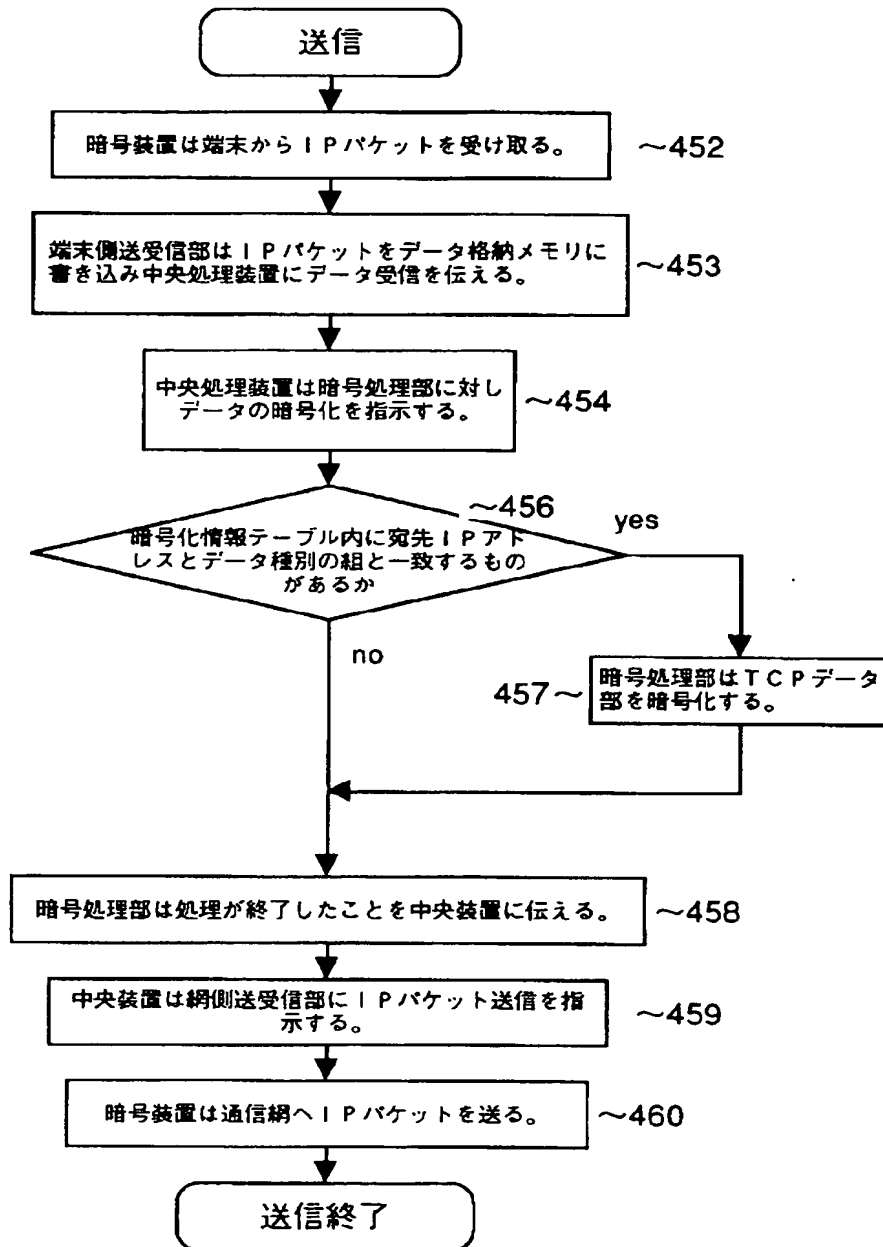
  

通信相手 IPアドレス	送信用 暗号鍵	受信用 暗号鍵	2d 暗号化情報 テーブル
31e	341n	341m	

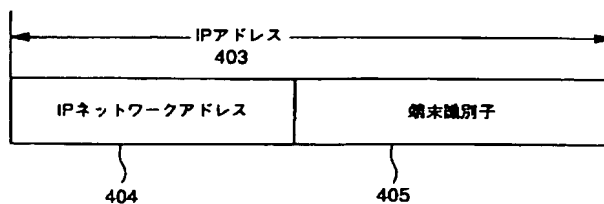
  

通信相手 IPアドレス	送信用 暗号鍵	受信用 暗号鍵	2e 暗号化情報 テーブル
31d	341m	341n	

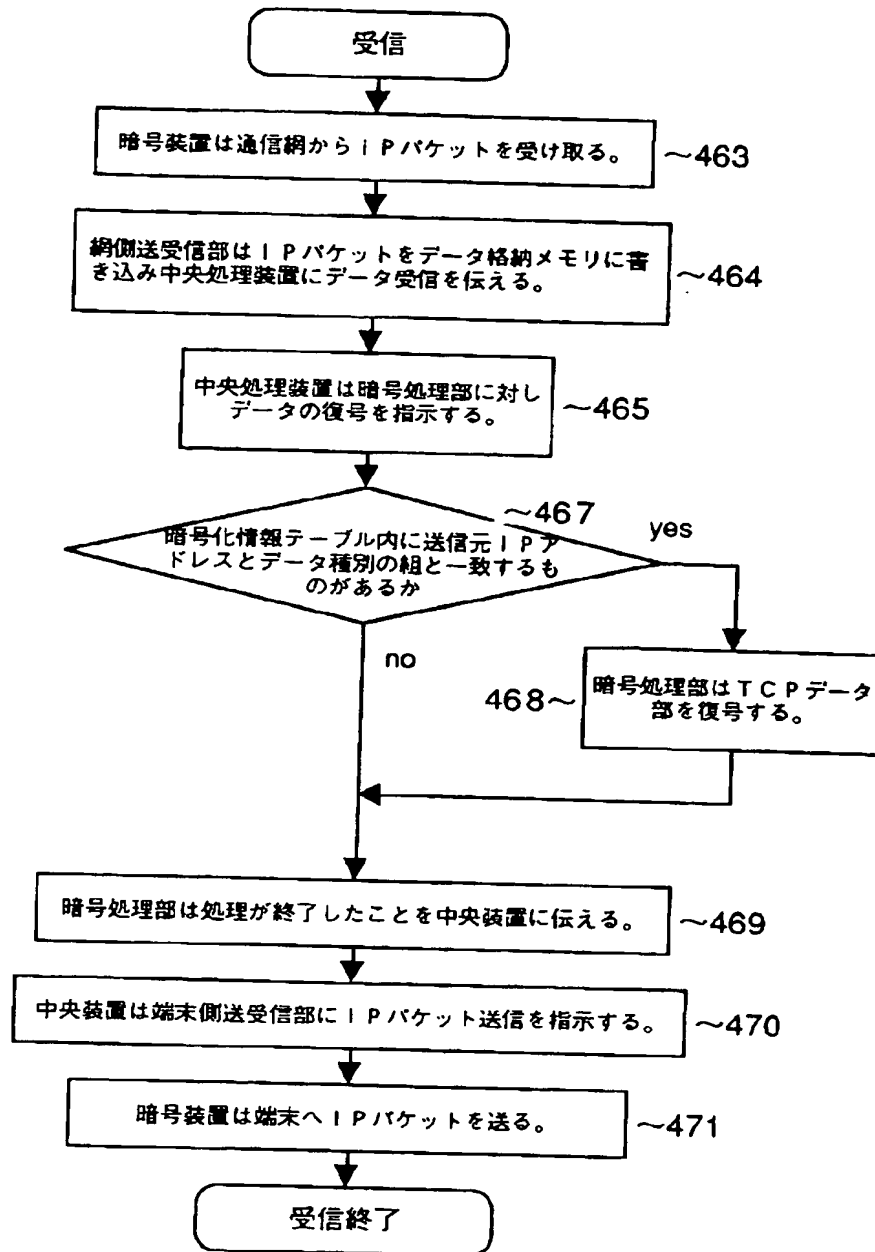
【図 5】



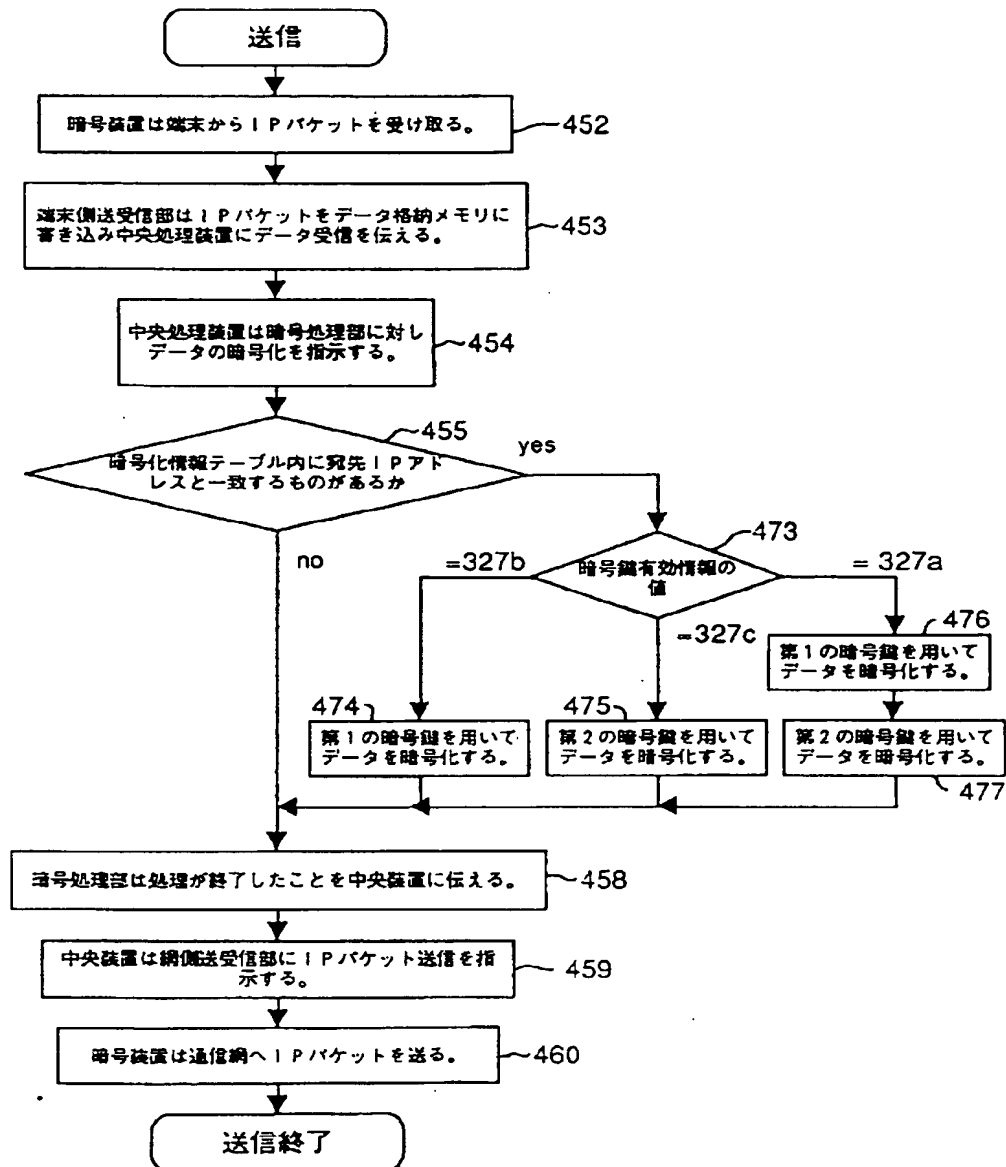
【図 18】



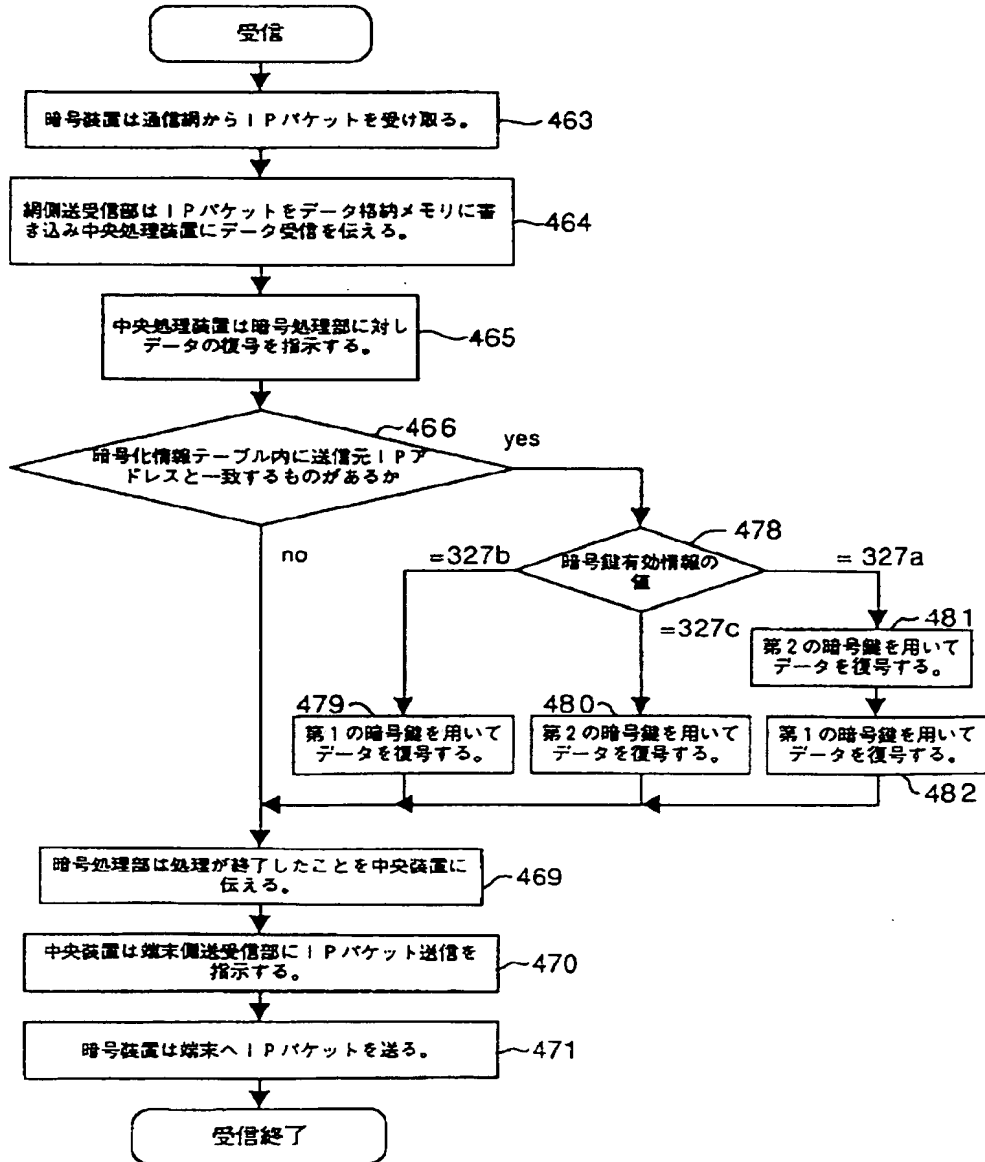
【図 6】



【図 8】

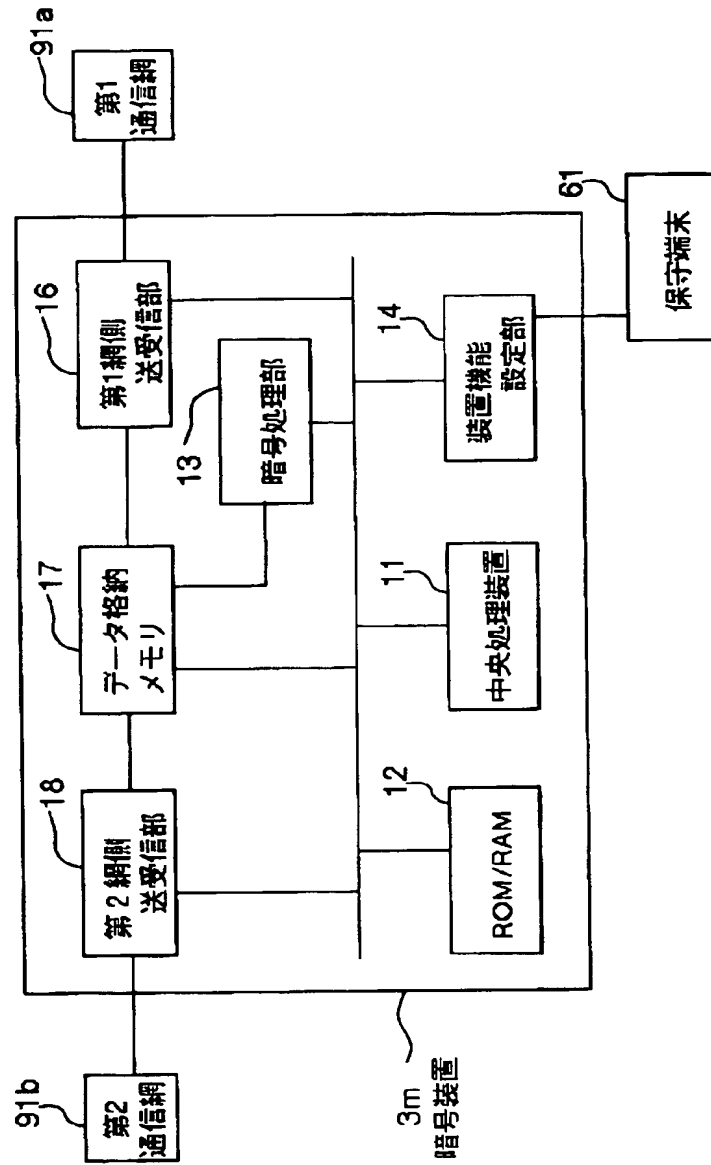


【図 9】

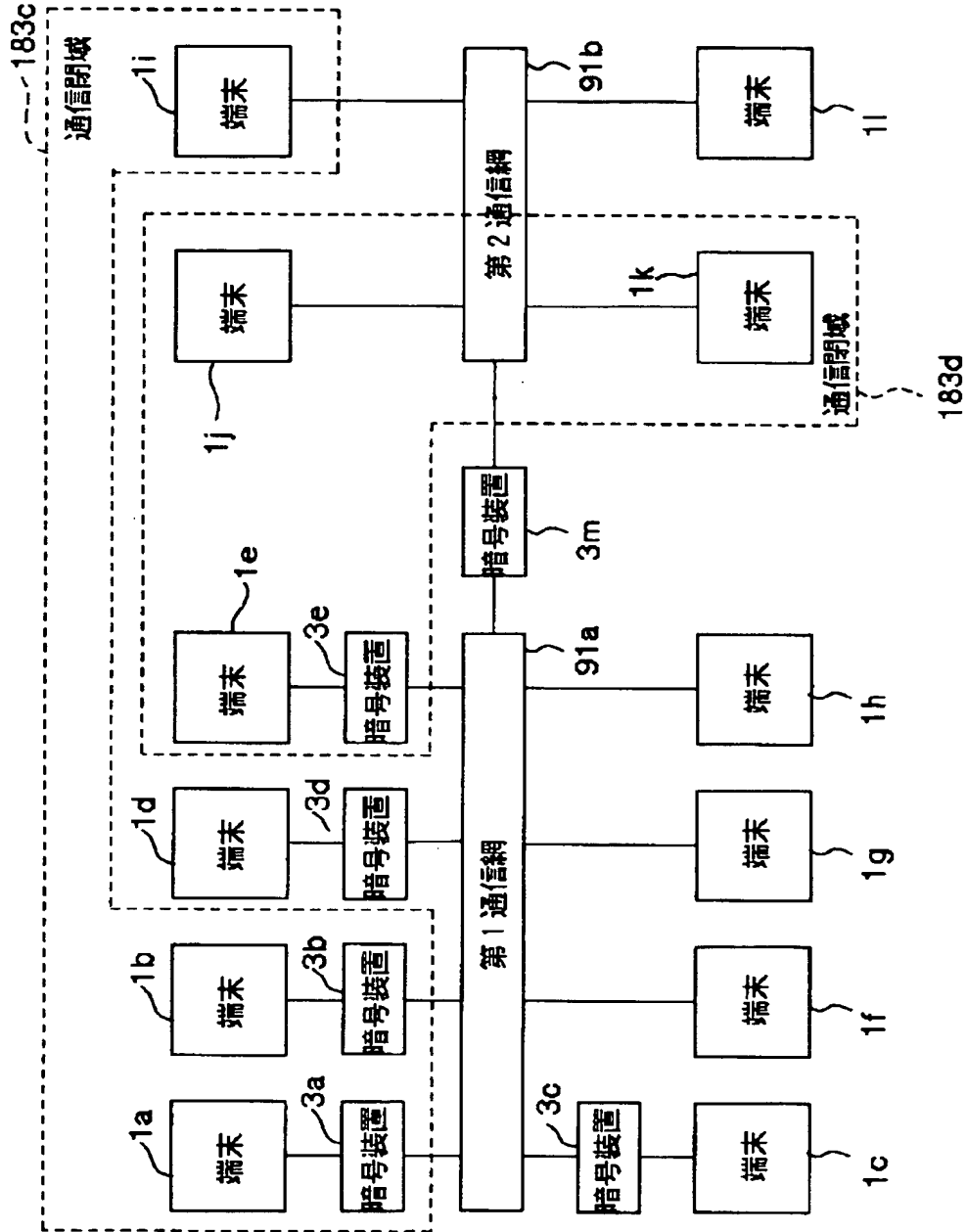




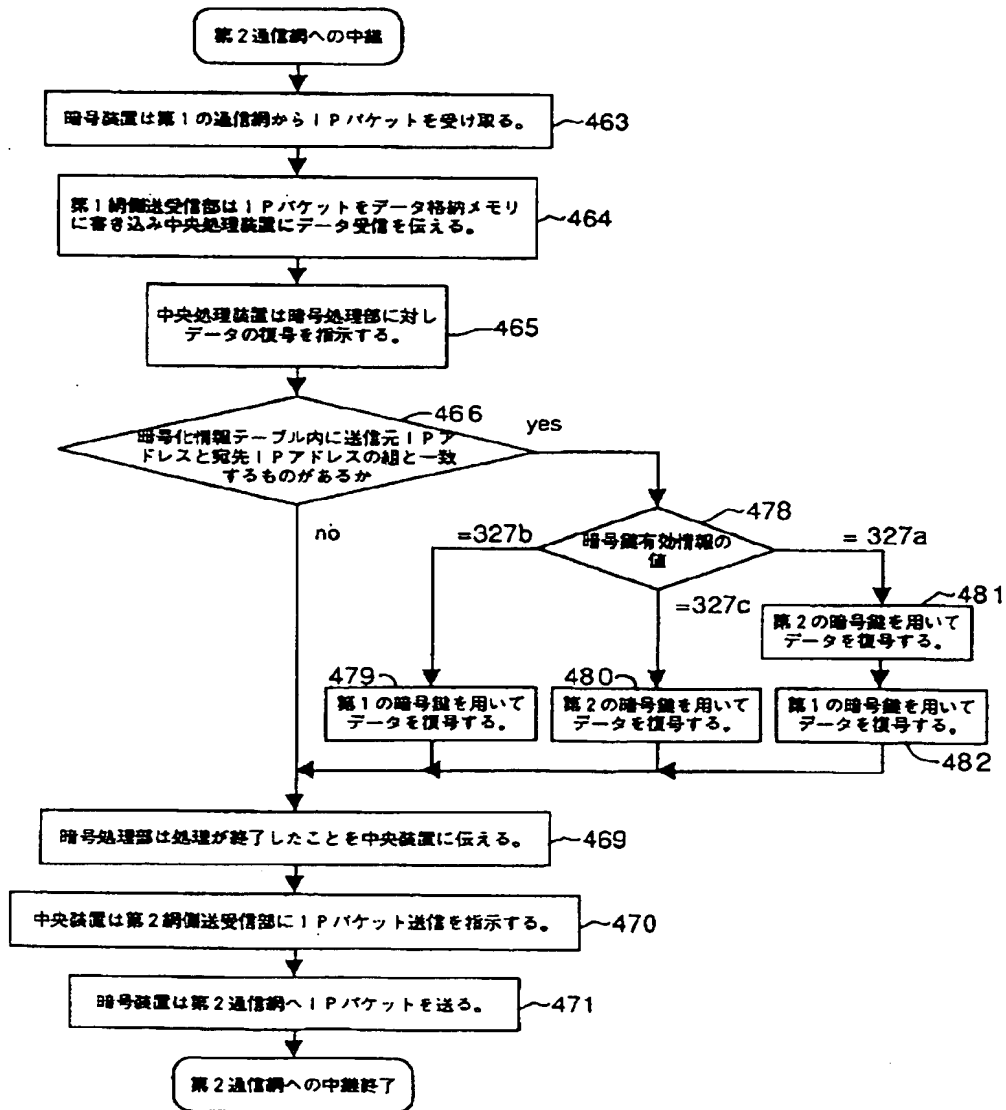
【図10】



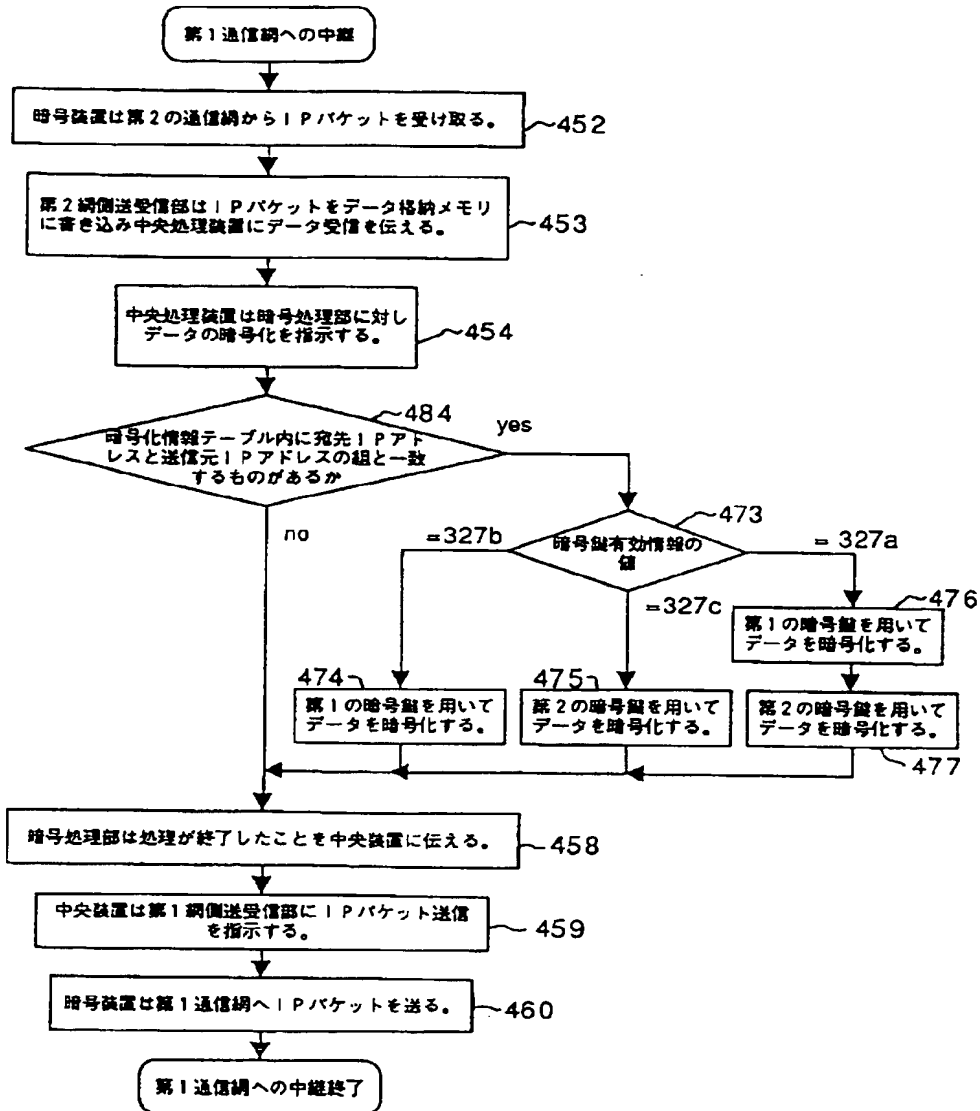
【図11】



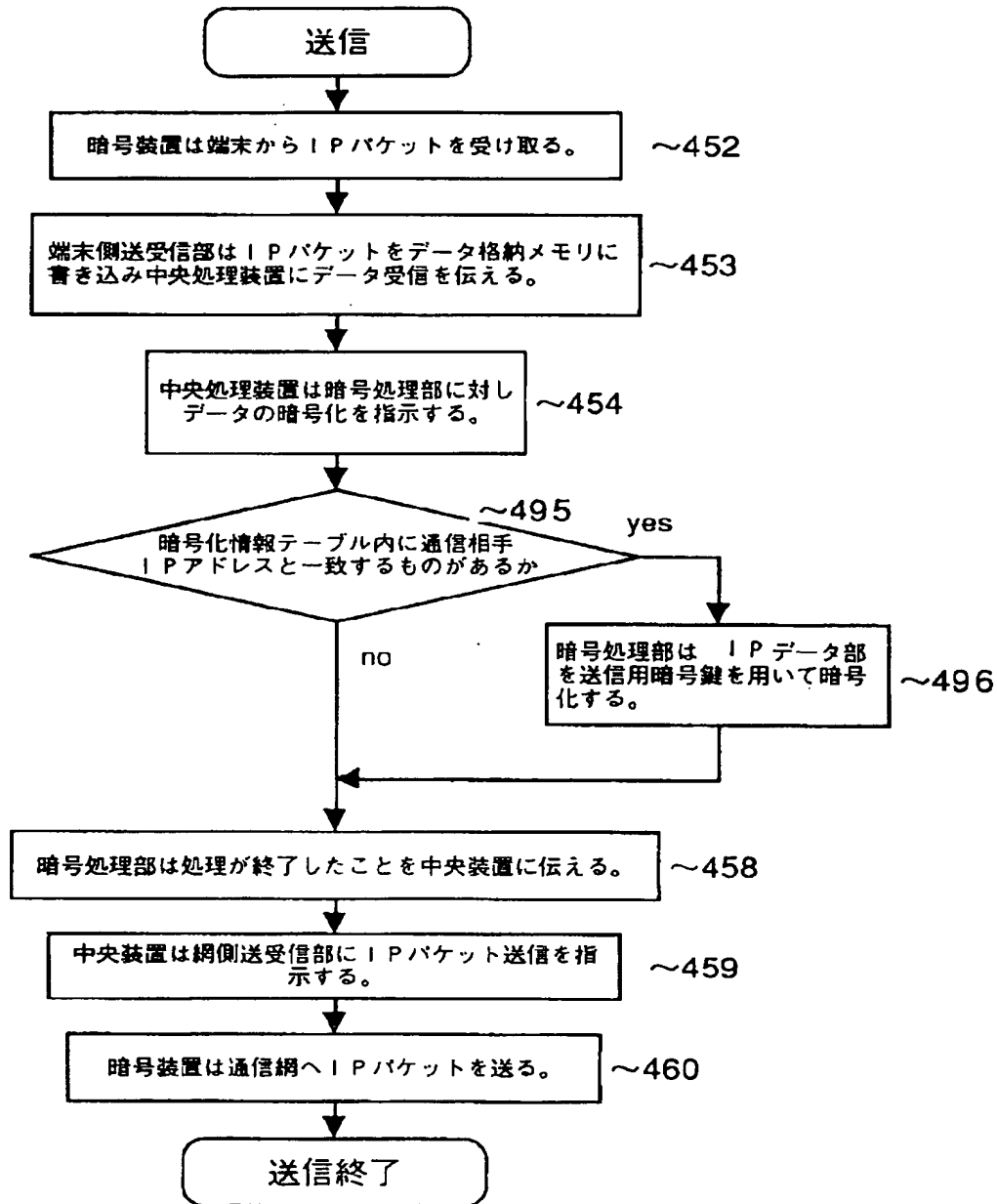
【図 13】



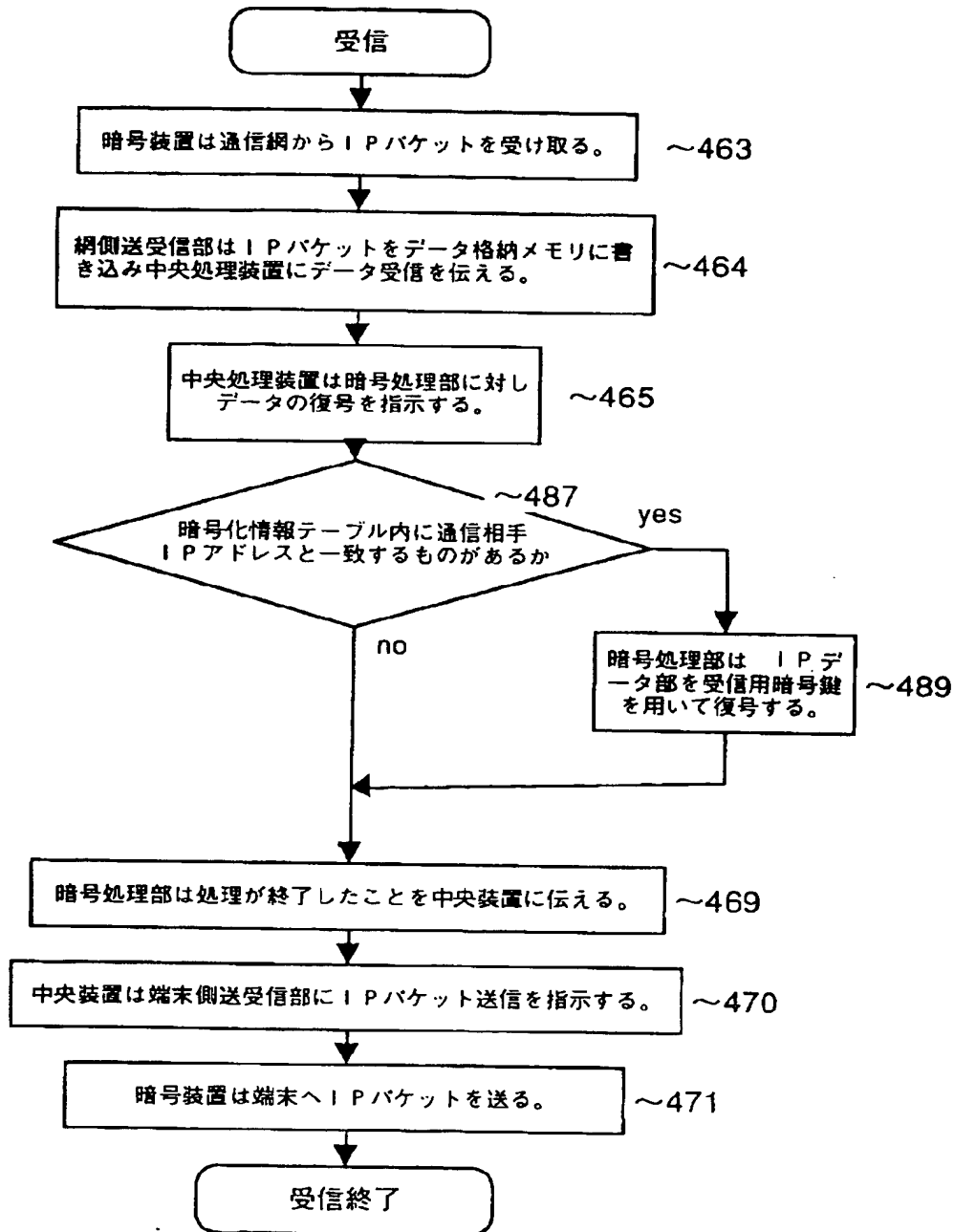
【図 14】



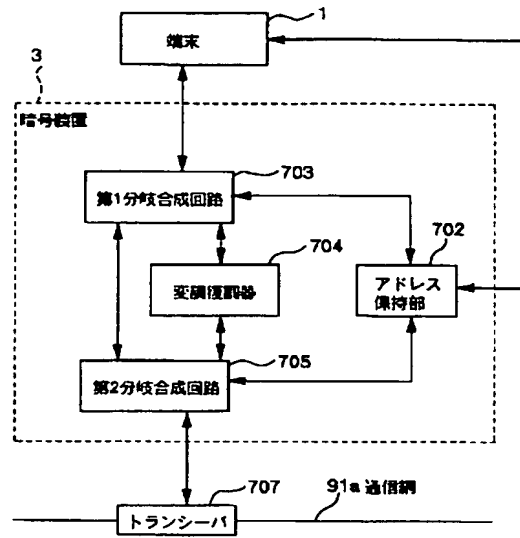
【図 16】



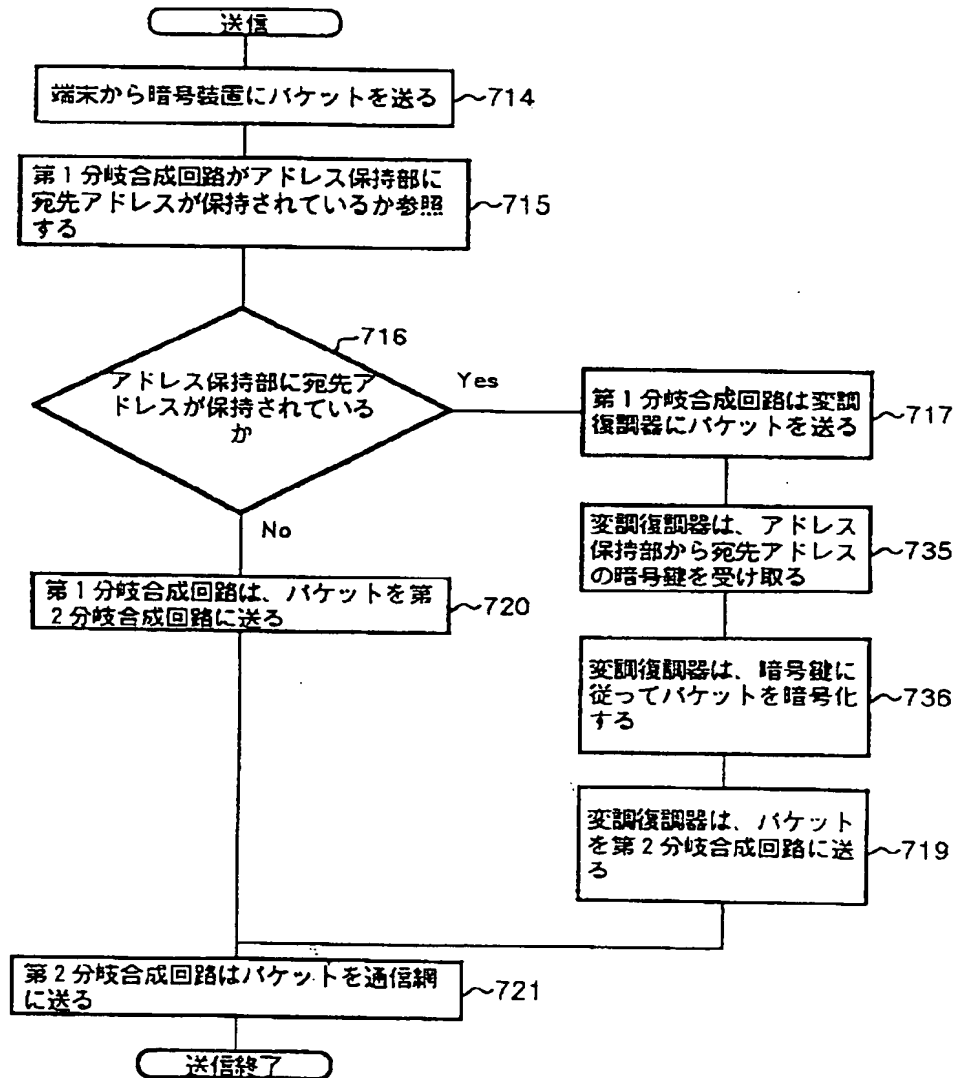
【図 17】



【図 1 9】

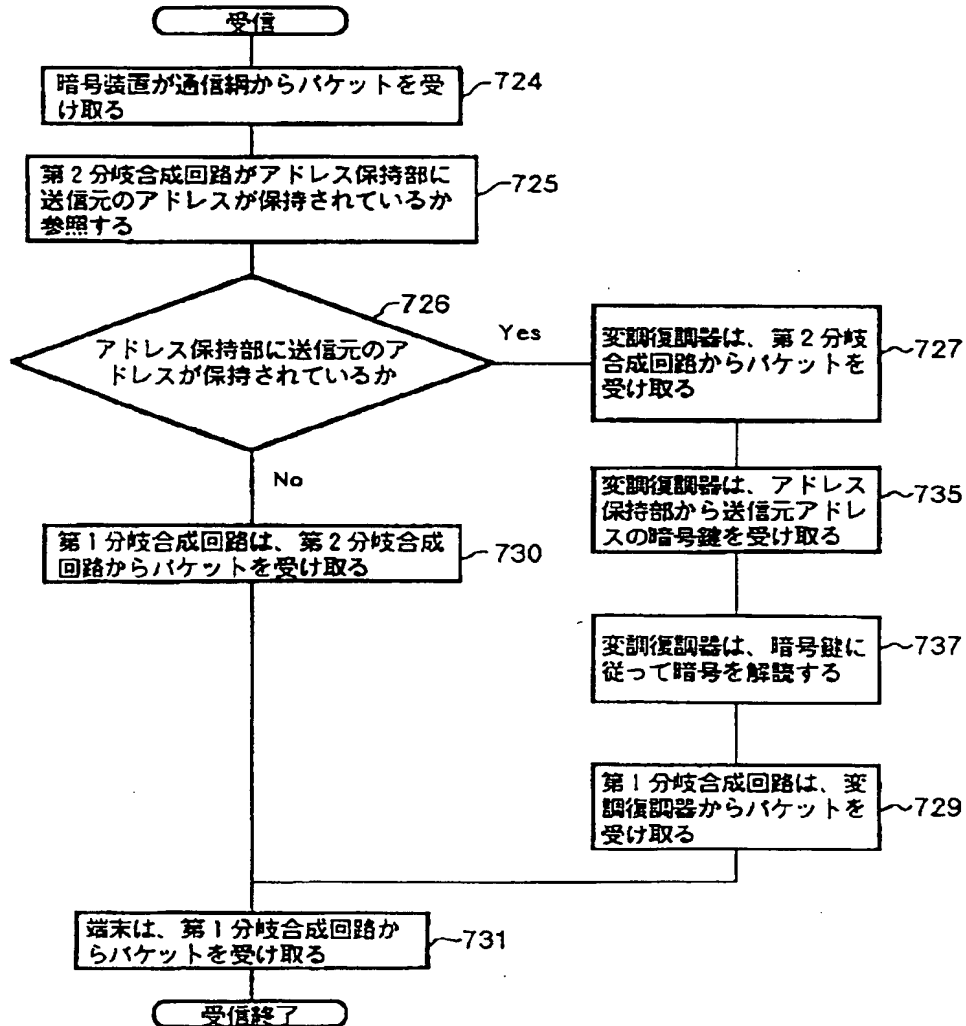


【図20】





【図 21】



フロントページの続き

(51) Int. Cl.<sup>6</sup>  
G 0 9 C 1/00識別記号 庁内整理番号  
7259-5 J

F I

技術表示箇所

(72) 発明者 横山 幸雄  
鎌倉市大船五丁目1番1号 三菱電機株式  
会社通信システム研究所内(72) 発明者 永島 規充  
鎌倉市大船五丁目1番1号 三菱電機株式  
会社通信システム研究所内